DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

HP INVENT – MANUAL APÊNDICES GR A HU

2003
PASTA 13

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 001
3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 002
3698
Doc.

translate lat

To translate a connection request to another protocol connection type when receiving a local-area transport (LAT) request, use the **translate lat** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate lat *incoming-service-name* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

no translate lat *incoming-service-name* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

incoming-service-name	A LAT service name. When used on the incoming portion of the command, *incoming-service-name* is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but is not required to. This argument is useful when making remote translated connections.
incoming-options	(Optional) An incoming connection request option. For LAT, the only option currently supported is: • **unadvertised**—Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
protocol outgoing-address	A protocol name followed by an address or host name. Protocol translation choices are: **ppp**, **slip**, **tcp**, and **x25**. **Note** The host name is resolved to an address during configuration, unless you are translating to TCP and use the **host-name** keyword, which allows the host name to be resolved at connection time instead of configuration time. See Table 38 for more information about the **host-name** keyword. Additional keywords that can be entered with the protocol are as follows: • **autocommand**—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the **autocommand** command. If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (" ") around the string.

8651
A

If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the **autocommand arap** keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string.

- **virtual-template**—Associates a virtual template with a virtual access interface. See the **translate lat (virtual access interfaces)** command description for more information.

outgoing-options	(Optional) Outgoing connection request options. Choices depend upon the protocol or command entered. See Table 36, Table 37, Table 38, and Table 39 for more information.
global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages.

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **no-reset** permanent virtual circuits (PVC) subkeyword was added to support outgoing PVCs.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. A LAT protocol translation command can be as simple as the following example:

```
Router(config)# translate lat LAT-1 X.25 1236672
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. Table 36, Table 37, Table 38, and Table 39 list the **translate lat** translation options by protocol.

RDS nº 03/2006 - CN - CPMI - CORREIOS
004
Fls. Nº 3698
Doc:

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate lat ?

  WORD  LAT service name

Router(config)# translate lat LSVC ?

  autocommand       Associate a command with a translation on this connections
  lat               DEC LAT protocol
  ppp               Virtual async PPP
  slip              Virtual async SLIP
  tcp               TCP/IP Telnet
  unadvertised      Prevent service advertisements from being broadcast to the
                    network
  virtual-template  Associate a virtual template with virtual access interface
  x25               X.25

Router(config)# translate lat LSVC tcp ?

  Hostname or A.B.C.D  IP address

Router(config)# translate lat LSVC tcp 1.1.1.1 ?

  access-class      Allow access list parameters to be used by source hosts
  binary            Negotiate Telnet binary mode on the connection
  host-name         Store the host name rather than its IP address
  local             Allow Telnet protocol negotiations not to be translated
  login             Require that the user log in before the outgoing connection
                    is made
  max-users         Limit the number of simultaneous users of the translation
  multibyte-IAC     Always treat multiple IACs as telnet command
  port              Port Number
  quiet             Suppress printing of user-information messages
  source-interface  Specify source interface
  stream            Treat telnet escape characters as data
```

Note If you plan to translate to X.25 on a permanent virtual circuit (PVC), see the description for the **translate x25** command for important configuration notes.

Table 36 LAT-to-PPP Outgoing Translation Options

Outgoing PPP Translation

ppp {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from LAT to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

3649
A-

Table 36 LAT-to-PPP Outgoing Translation Options (continued)

Outgoing PPP Connection Request Options

Add any of the following keywords to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both keywords, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression**—Implements header compression on IP packets only.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

Table 37 LAT-to-SLIP Outgoing Translation Options

Outgoing SLIP Translation

slip {*ip-address*| **ip-pool** [**scope-name** *name*]}

Translates from LAT to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

RDS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0006
3698

8648

Table 37 LAT-to-SLIP Outgoing Translation Options (continued)

Outgoing SLIP Connection Request Options

Add any of the following keywords to configure SLIP connection requests:

- **header-compression [passive]**—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Table 38 LAT-to-TCP Outgoing Options

Outgoing TCP Translation

tcp *ip-address*

Translates LAT to TCP/IP Telnet. Supply an IP address as a standard, four-part dotted decimal IP address, the name of an IP host that can be resolved by the DNS, or explicit specification in an **ip host** command (refer to the description for the **host-name** keyword in the "Outgoing TCP Connection Request Options" section).

Outgoing TCP Connection Request Options

Any of the following optional keywords can be used to configure TCP connection requests:

- **binary**—Negotiates Telnet binary mode on the connection.
- **host-name**—Stores the host name rather than its IP address, thereby allowing the host name to be resolved at connection time instead of configuration time. There is also a **rotor** keyword suboption that you can use to modify the behavior of the **host-name** keyword by allowing one of the IP addresses defined by the **ip host** configuration command to be chosen randomly. If one address fails, another one will be tried, and so on until all address choices are exhausted. You can use the **rotor** keyword, therefore, to provide basic load sharing of the IP destinations.
- **multibyte-IAC**—Always treat multiple Interpret as Command (IAC) escape character codes as a Telnet command.
- **port** *number*—For outgoing connections, enter the number of the port to match. The default is port 23 (Telnet).

ECT 03/2006 - CN - CPMI - CORREIOS
Fls. Nº 007
3698
Doc:

8647
A.

Table 38 LAT-to-TCP Outgoing Options (continued)

- **source-interface**—Specifies the source address used for Telnet connections initiated by the router.
- **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

Table 39 LAT-to-X.25 Outgoing Translation Options

Outgoing X.25 Translation

x25 *x.121-address*

Translates LAT to the X.25 protocol. Supply an X.121 address that conforms to the specifications provided in the *CCITT 1984 Red Book*, or the name of an X.25 host that can be resolved by the DNS, or explicit specification in an **x25 host** command.

The address number generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.

Outgoing X.25 Connection Request Options

Any of the following optional keywords can be used to configure X.25 connection requests:

- **cud** *c-u-data*—Sends the specified X.25 Call User Data (CUD) text as part of an outgoing call request after the protocol identification bytes.
- **no-reverse**—Specifies that outgoing calls not request the X.25 reverse charge facility, when the interface default is that all outgoing calls are reverse charged.
- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size* | **no-reset**]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.
  - **no-reset**—Causes the Cisco router to send a no Reset packet request at startup of a TCP or LAT to permanent virtual circuit (PVC) translation session.

008
3698

8646
A.

Table 39 LAT-to-X.25 Outgoing Translation Options (continued)

- **reverse**—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls.
- **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. When the **use-map** keyword is specified on the **translate** command, the Destination address and optional PAD Protocol Identification (PID), CUD, and facilities are checked against a configured list of **x25 map pad** entries. If a match is found, the map entry PID, CUD, and facilities are applied to the outgoing protocol translation call. The X.25 map facilities applied to the outgoing translation can be displayed with the **show translation** command throughout the duration of the translation session.

Examples

The following example illustrates incoming LAT to outgoing TCP translations. The **unadvertised** keyword prevents broadcast of service advertisements to other servers in the network. Outgoing translated packets are sent to IP host Host1, TCP port 4005.

```
translate lat pt-printer1 unadvertised tcp Host1 port 4005
```

The following example translates LAT on an incoming line to SLIP on an outgoing line. It uses header compression only if incoming TCP packets on the same interface are compressed.

```
translate lat Service1 slip 10.0.0.4 header-compression
```

The following example first shows how to disable keepalive packets on a PPP line using the **translate lat** command, then shows translated session output from the **show translate** EXEC command indicating keepalive packets have been turned off.

```
translate lat Service2 ppp 172.21.2.2 keepalive 0
.
.
.
Router# show translate

Translate From: LAT Service2
          To:   PPP 172.21.2.2 keepalive 0
          0/0 users active, 0 peak, 0 total, 0 failures
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

CPMI - CORRESP
Pg. N° 009
Doc. 3698

8645
A-

translate lat (virtual access interfaces)

When receiving a local-area transport (LAT) connection request to a service name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate lat** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template. Table 40 lists all outgoing options and their corresponding interface configuration commands.

translate lat *incoming-service-name* [*incoming-options*] **virtual-template** *number* [*global-options*]

no translate lat *incoming-service-name* [*incoming-options*] **virtual-template** *number* [*global-options*]

Syntax Description

incoming-service-name	A LAT service name. When used on the incoming portion of the **translate lat** command, *service-name* is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but this match is not required. Such matches can be useful when making remote translated connections.
incoming-options	(Optional) An incoming connection request option. For LAT, the only keyword currently supported is: • **unadvertised**—Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
virtual-template *number*	Applies the virtual interface template specified by the *number* argument in place of outgoing options.
global-options	(Optional) Translation options that can be used by any connection type and can be one or more of the following: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **quiet**—Suppresses printing of user-information messages.

CPMI - CORREIOS
010
3698

8644
A.

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address, host name, or service name. The protocol connection information is followed by optional features for that connection, as appropriate. For example, the **binary** keyword is only appropriate with TCP/IP connections. The global options, in general, apply to all the connection types, but there are exceptions.

Rather than specifying outgoing translation options in the **translate** command, configure these options as interface configuration commands under the virtual interface template, then apply the virtual interface template to the **translate** command. Table 40 maps outgoing **translate** command options to interface commands you can configure in the virtual interface template.

Table 40 Mapping Outgoing translate lat Options to Interface Commands

translate lat Command Options	Corresponding Interface Configuration Command
ip-pool	**peer default ip address** {**ip-address** | **dhcp** | **pool** [*poolname*]}
header-compression	**ip tcp header compression** [**on** | **off** | **passive**]
routing	**ip routing** or **ipx routing**
mtu	**mtu**
keepalive	**keepalive**
authentication {**chap** | **pap**}	**ppp authentication** {**chap** | **pap**}
ppp use-tacacs	**ppp use-tacacs**
ipx loopback	**ipx ppp-client loopback** *number*

Examples

The following example configures PPP tunneling from a PC across a LAT network. The remote PC is given the IP address 10.12.118.12 when it dials in. The **unadvertised** keyword prevents broadcast of service advertisements to other servers.

```
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 10.12.118.12
 ppp authentication chap
!
translate lat pt-printer1 unadvertised virtual-template 1
```


011
3698

8643
A.

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 012
3698
Doc:

translate tcp

To translate a connection request to another protocol connection type when receiving a TCP connection request to a particular destination address or host name, use the **translate tcp** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate tcp *incoming-address* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

no translate tcp *incoming-address* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

incoming-address	Standard IP address in standard, four-part dotted decimal notation. The IP address cannot be in use by other routers, and it should be on a connected subnet.
incoming-options	(Optional) An incoming connection request option. Choices are as follows: • **binary**—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the protocol translation software and is set automatically when you enter a **translate** command in the previous format.) • **port** *number*—The number of the port to match for incoming connections. The default is port 23 (Telnet). For outgoing connections, enter the number of the port to use. The default is port 23. • **printer**—Supports local-area transport (LAT) and X.25 printing over a TCP network among multiple sites. This keyword causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation. • **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

8640
A.

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **no-reset** permanent virtual circuits (PVCs) subkeyword was added to support outgoing PVCs.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. A TCP protocol translation command can be as simple as the following example:

```
Router(config)# translate tcp 10.1.1.1 X.25 1236672
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. Table 41, Table 42, Table 43, and Table 44 list the **translate tcp** translation options by protocol.

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate tcp ?

  Hostname or A.B.C.D  IP address

Router(config)# translate tcp 1.1.1.1 ?

  autocommand       Associate a command with a translation on this connections
  binary            Negotiate Telnet binary mode on the connection
  lat               DEC LAT protocol
  port              Port Number
  ppp               Virtual async PPP
  printer           Enable non-interactive (implies global quiet)
  slip              Virtual async SLIP
  stream            Enable stream processing
  tcp               TCP/IP Telnet
  virtual-template  Associate a virtual template with virtual access interface
  x25               X.25

Router(config)# translate tcp 1.1.1.1 lat LAT-1 ?

  access-class  Allow access list parameters to be used by source hosts
  local         Allow Telnet protocol negotiations not to be translated
  login         Require that the user log in before the outgoing connection is
                made
  max-users     Limit the number of simultaneous users of the translation
  node          LAT node name
  port          LAT port name
  quiet         Suppress printing of user-information messages
  unadvertised  Prevent service advertisements from being broadcast to the
                network
```

Note If you plan to translate to X.25 on a permanent virtual circuit (PVC), see the description for the translate x25 command for important configuration notes.

ROS nº 09XXX - FN - CORREIOS
Fls. Nº 014
3698
Doc.

8635
A

Table 41 TCP-to-LAT Outgoing Options

Outgoing LAT Translation

lat *service-name*

Translates TCP to the LAT protocol.The software must learn the service name through LAT service advertisements before it can use the service.

Outgoing LAT Connection Request Options

Any of the following optional keywords can be used to configure LAT connection requests:

- **node** *name*—Connects to the specified node that offers a LAT service. By default, the connection is made to the highest-rated node that offers the service.
- **port** *name*—Destination LAT port name in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.
- **unadvertised**—Prevents LAT service advertisements from being broadcast to the network.

Table 42 TCP-to-PPP Outgoing Options

Outgoing PPP Translation

ppp {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from TCP to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Any of the following optional keywords can be used to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both keywords, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.

FPMI - CONGRES
FIS—N° 015
3698
Doc.

8638
A.

Table 42 TCP-to-PPP Outgoing Options (continued)

- **mtu** *bytes*—Sets the interface maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

Table 43 TCP-to-SLIP Outgoing Options

Outgoing SLIP Translation

slip {*ip-address* | **ip-pool** [**scope-name** *name*]}

Translates from TCP to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** keyword applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Outgoing SLIP Connection Request Options

Any of the following optional keywords can be used to configure SLIP connection requests:

- **header-compression [passive]**—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Fls. Nº 016
3698
Doc:

8637
A.

Table 44 TCP-to-X.25 Outgoing Options

Outgoing X.25 Translation

x25 *x.121-address*

Translates TCP to the X.25 protocol. Supply an X.121 address that conforms to the specifications provided in the *CCITT 1984 Red Book*, or the name of an X.25 host that can be resolved by the DNS, or explicit specification in an **x25 host** command.

The address number generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.

Outgoing X.25 Connection Request Options

Any of the following optional keywords can be used to configure X.25 connection requests:

- **cud** *c-u-data*—Sends the specified X.25 Call User Data (CUD) text as part of an outgoing call request after the protocol identification bytes.
- **no-reverse**—Specifies that outgoing calls not request the X.25 reverse charge facility, when the interface default is that all outgoing calls are reverse charged.
- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* **[interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size* | **no-reset]**—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the incoming connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.
  - **no-reset**—Causes the Cisco router to send a no Reset packet request at startup of a TCP or LAT to PVC translation session.
- **reverse**—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls.
- **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. When the **use-map** keyword is specified on the **translate** command, the Destination address and optional PAD Protocol Identification (PID), CUD, and facilities are checked against a configured list of **x25 map pad** command entries. If a match is found, the map entry PID, CUD, and facilities are applied to the outgoing protocol translation call. The X.25 map facilities applied to the outgoing translation can be displayed with the **show translation** command throughout the duration of the translation session.

ECT/DEINF/COS - CN - CPMI - CORREIOS
Fls. Nº 017
3698
Doc:

8036
A.

Examples

The following example illustrates the use of the TCP incoming protocol **printer** keyword for an incoming TCP connection:

```
translate tcp 172.19.32.250 printer x25 5678
```

The following example permits clients running IPX-PPP to connect through the device virtual terminal lines to a server running PPP:

```
interface loopback0
  no ip address
  ipx network 544
  ipx sap-interval 2000
!
translate tcp 172.21.14.67 port 1234 ppp 10.0.0.2 ipx loopback0
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
018
Fls Nº
Doc: 3698

8635
A.

translate tcp (virtual access interfaces)

When receiving a TCP connection request to a particular destination address or host name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate tcp** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template.

translate tcp *incoming-address* [*incoming-options*] **virtual-template** *number* [*global-options*]

no translate tcp *incoming-address* [*incoming-options*] **virtual-template** *number* [*global-options*]

Syntax Description

incoming-address	TCP/IP Telnet and a standard IP address or host name. The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an **ip host** command.
incoming-options	(Optional) Incoming connection request options. These arguments can have the following values: • **binary**—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the Cisco IOS software and is set automatically when you enter a **translate** command in the old format.) • **port** *number*—For incoming connections, enter the number of the port to match. The default is port 23 (Telnet). For outgoing connections, enter the number of the port to use. The default is port 23. • **printer**—Supports LAT and X.25 printing over a TCP network among multiple sites. This keyword causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation. • **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.
virtual-template *number*	Applies the virtual interface template specified by the *number* argument in place of outgoing options.

File N° 019
Doc 3698

3634
A.

global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Maximum number of simultaneous users of the translation. • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for TCP-to-X.25 translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address, host name, or service name. The protocol connection information is followed by optional features for that connection, as appropriate. For example, the **binary** keyword is only appropriate with TCP/IP connections. The global options, in general, apply to all the connection types, but there are exceptions.

Examples

The following example illustrates the use of the TCP incoming **printer** keyword for an incoming TCP connection:

```
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 10.12.108.1
 ppp authentication chap

translate tcp 172.19.32.250 printer Virtual-Template1
```


Fls Nº 020
Doc 3698

8633
A.

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

CPMI - CORREIOS
Fls. Nº 021
Doc. 3698

8632
A.

translate x25

To translate a connection request to another protocol connection type when receiving an X.25 connection request to a particular destination address or host name, use the **translate x25** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

no translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

incoming-address	An X.25 and X.121 address that conform to specifications provided in the *CCITT 1984 Red Book.* This address generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.
incoming-options	(Optional) An incoming connection request option. Choices are as follows: • **accept-reverse**—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. • **cud** *c-u-data*—Specifies the Call User Data (CUD) field to match in the X.25 Incoming Call packet. If not configured, the CUD in the Incoming Call packet must be blank. • **idle** *minutes*—Specifies the number of minutes the virtual circuit is idle. This keyword enables the protocol translation function to clear a switched virtual circuit after a set period of inactivity, where *minutes* is the number of minutes in the period. Calls either originated or terminated are cleared. The maximum value of *minutes* is 255. The default value of *minutes* is zero. • **printer**—Supports local-area transport (LAT) and TCP printing over an X.25 network among multiple sites. Provides an "interlock mechanism" between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. This keyword causes the Cisco IOS software to delay the call confirmation of an incoming X.25 call request until after the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation.

022
3698

8631
A.

- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size*]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are as follows: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.

protocol outgoing-address

A protocol name followed by an address or host name. Protocol translation choices are **lat**, **ppp**, **slip**, and **tcp**.

Note The host name is translated to an address during configuration, unless you are translating to TCP and use the **host-name** keyword, which allows the host name to be resolved at connection time instead of configuration time. See Table 48 for more information about the **host-name** keyword.

Additional keywords that can be entered with the protocol are as follows:

- **autocommand**—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the **autocommand** keyword. If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (" ") around the string. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the **autocommand arap** keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string.
- **virtual-template**—Associates a virtual template with a virtual access interface. See the translate x25 (virtual access interfaces) command description for more information.

CORREIOS
Fls. Nº 023
3698
Doc

8630
A.

outgoing-options	(Optional) Outgoing connection request option. Choices depend upon the protocol or command entered. See Table 45,Table 46, Table 47, and Table 48 for a list of outgoing protocol translation options.
global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for X.25-to-TCP translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. An X.25 protocol translation command can be as simple as the following example:

```
Router(config)# translate X.25 1236672 tcp 1.1.1.1
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. Table 45, Table 46, Table 47, and Table 48 lists the **translate x25** translation options by protocol.

024

8629
A

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate x25 ?

  WORD  X.121 Address pattern

Router(config)# translate x25 66666 ?

  accept-reverse    Accept reverse charge on a per-call basis
  autocommand       Associate a command with a translation on this connections
  cud               Specify the Call User Data (CUD)
  idle              Specify VC idle timer
  lat               DEC LAT protocol
  ppp               Virtual async PPP
  printer           Enable non-interactive (implies global quiet)
  profile           Use a defined X.3 profile
  pvc               An incoming connection is actually a PVC
  slip              Virtual async SLIP
  tcp               TCP/IP Telnet
  virtual-template  Associate a virtual template with virtual access interface
  x25               X.25

Router(config)# translate x25 66666 tcp 1.1.1.1 ?

  access-class      Allow access list parameters to be used by source hosts
  binary            Negotiate Telnet binary mode on the connection
  host-name         Store the host name rather than its IP address
  local             Allow Telnet protocol negotiations not to be translated
  login             Require that the user log in before the outgoing connection
                    is made
  max-users         Limit the number of simultaneous users of the translation
  multibyte-IAC     Always treat multiple IACs as telnet command
  port              Port Number
  quiet             Suppress printing of user-information messages
  source-interface  Specify source interface
  stream            Treat telnet escape characters as data
  swap              Allow X.3 parameters to be set on the protocol translator
                    by the host originating the X.25 call
```

Table 45 X.25-to-LAT Outgoing Options

Outgoing LAT Translation

lat *service-name*

Translates X.25 to the LAT protocol.The software must learn the service name through LAT service advertisements before it can use the service.

Outgoing LAT Connection Request Options

Any of the following optional keywords can be used to configure LAT connection requests:

- **node** *name*—Connects to the specified node that offers a LAT service. By default, the connection is made to the highest-rated node that offers the service.
- **port** *name*—Destination LAT port name in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.
- **unadvertised**—Prevents LAT service advertisements from being broadcast to the network.

CPMI - CORREIOS
Fls Nº 665
Doc 3698

3628
A-

Table 46 X.25-to-PPP Outgoing Options

Outgoing PPP Translation

ppp {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from X.25 to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Any of the following optional keywords can be used to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both options, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression**—Configures header compression on IP packets only.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This option is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

026
3698

8627
A.

Table 47 X.25-to-SLIP Outgoing Options

Outgoing SLIP Translation

slip {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from X.25 to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Outgoing SLIP Connection Request Options

Any of the following optional keywords can be used to configure SLIP connection requests:

- **header-compression [passive]**—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Table 48 X.25-to-TCP Outgoing Options

Outgoing TCP Translation

tcp *ip-address*

Translates X.25 to TCP/IP Telnet. Supply an IP address as a standard, four-part dotted decimal IP address, or the name of an IP host that can be resolved by the DNS, or explicit specification in an **ip host** command (refer to the description for the **host-name** keyword in the "Outgoing TCP Connection Request Options" section).

FLS 627
3698

Table 48 X.25-to-TCP Outgoing Options (continued)

Outgoing TCP Connection Request Options

Any of the following optional keywords can be used to configure TCP connection requests:

- **binary**—Negotiates Telnet binary mode on the connection.
- **host-name**—Stores the host name rather than its IP address, thereby allowing the host name to be resolved at connection time instead of configuration time. There is also a **rotor** keyword suboption that you can use to modify the behavior of the **host-name** keyword by allowing one of the IP addresses defined by the **ip host** configuration command to be chosen randomly. If one address fails, another one will be tried, and so on until all address choices are exhausted. You can use the **rotor** keyword, therefore, to provide basic load sharing of the IP destinations.
- **multibyte-IAC**—Always treat multiple Interpret as Command (IAC) escape character codes as a Telnet command.
- **port** *number*—For incoming connections, enter the number of the port to match. The default is port 23 (Telnet).
- **source-interface**—Specifies the source address used for Telnet connections initiated by the router.
- **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This option might be useful for connections to ports running UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

Protocol Translation and X.25 PVCs Functional Description

This section describes how the protocol translator works with X.25 PVCs. It will help you understand the overall behavior of incoming and outgoing X.25 PVCs associated with a **translate** command, enabling you to correctly configure protocol translator PVCs for your application.

Configuring X.25 PVCs

When the **translate x25** command is configured with a PVC, an attempt is made to create the PVC. The following conditions can cause this attempt to fail:

- The PVCs assignment of the X.25 interface does not include the PVC number in the **translate x25** command.
- The PVC number in the **translate x25** command is already in use.
- An X.25 destination in a **translate x25** command is routed to X.25 over TCP/IP (XOT), Connection Mode Network Service (CMNS), or Annex G, which do not support translated PVCs.

PVC numbers must be unique across an X.25 connection; however, PVC 1 on Serial 1/0 is different (and therefore unique) from PVC 1 on Serial 2/1.

If, once the **translate x25** command is accepted, the X.25 interface on which the PVC is created goes down, the PVC enters an inactive state, the TCP or LAT connection is terminated, but the existing PAD context remains inactive.

An incoming TCP or LAT connection associated with a down outgoing PVC (displaying a "P/Inactive message") will be rejected by the protocol translator.

If any X.25 traffic is received while the corresponding TCP or LAT connection is terminated, and if a Data packet is received in state D1, a Reset with a diagnostic message will be displayed, similar to the following:

```
20:17:11.809: Serial2: X.25 O D1 Reset (5) 8 lci 4
20:17:11.809: Cause 29, Diag 113 (Network out of order (PVC)/Remote network problem)
```

The number of outgoing and incoming protocol translation PVCs is limited only by the number of virtual terminal lines supported on the Cisco router. Remember that each protocol translation session uses a virtual terminal line, which lowers the number of virtual terminal lines available for Telnet sessions.

By default, the Cisco router sends a Reset packet with the cause "PVC Network Operational" and diagnostic "Maintenance action" messages at the start of a TCP or LAT to PVC translation session, to announce that the connection is established and that the PVC is able to handle data traffic. To suppress the PVC Reset packet at TCP or LAT session startup, configure the **no-reset** outgoing PVC keyword as shown in the following example:

```
translate tcp 192.168.22.102 port 5 x25 333 pvc 5 no-reset profile tcl
```

Changing or Removing a translate Command PVC Configuration

Removing a **translate** command with an outgoing PVC specified is allowed only when there no active connection is associated with the outgoing PVC. An attempt to remove an active translation results in the following message:

```
Translate: Can't delete/add entry - Connection(s) are currently active
```

For example, if PVC 5 is assigned to a **translate** command as shown in the following example:

```
translate tcp 10.0.155.61 port 5 x25 5 pvc 5 interface Serial2/0
```

And you want PVC 5 to be assigned under an X.25 interface instead of the **translate** command, as shown in the following example:

```
interface serial2/0
  x25 pvc 5 int s4/0 pvc 25
```

Perform the following steps to configure this reassignment:

Step 1 Check whether a PVC is associated with a serial connection using the **show x25** EXEC command, as follows:

```
Router# show x25 vc 5

PVC 5, State:D1, Interface:Serial2/0
   Started ...

   Line:230 vty 4  Location:Host:nmos3m1
    connected to PAD <--> X25
```

Step 2 If the PVC is associated with a TCP connection, terminate the connection by disconnecting the TCP session or by using the **clear line** EXEC command as shown in the following example:

```
Router# clear line vty 4
```

Step 3 Enter configuration mode, delete the **translate** command, and reassign PVC 5 to an interface:

```
Router(config)# no translate tcp 10.0.155.61 port 5 x25 5 pvc 5 interface Serial2/0
Router(config)# interface serial2/0
Router(config-if)# x25 pvc 5 int s4/0 pvc 25
```

If you want to modify the **translate** command and change the PVC number from 5 to 12, follow steps 1 and 2, and modify the **translate** command with PVC 12, as follows:

```
Router(config)# translate tcp 10.0.155.61 port 12 x25 12 pvc 12 interface Serial2/0
```

Understanding the X.25 Address and the PVC Interface Option on a translate Command

The protocol translator locates the X.121 destination address in the X.25 route table to determine the interface on which to establish the PVC. A more up-to-date, simpler approach uses the **translate** command with the **interface** keyword, which ignores the status of the interface by avoiding referencing the X.25 route table.

For example, instead of configuring an **x25 route** command for each translated PVC, and entering a long X.121 address on the **translate** command, as shown this example:

```
x25 route ^32785223344502 interface Serial1/5
translate tcp 10.0.155.61 port 2502 x25 32785223344502 pvc 1
```

You can simply enter one **translate** command that links the IP port number with the X.121 address and specifies the interface on which to establish the PVC, as follows:

```
translate tcp 10.0.155.61 port 2502 x25 2502 pvc 1 interface Serial 1/5
```

This is the recommended approach and should be adopted in place of **translate** commands that cause the destination address to be looked up in the route table.

Examples

The following example shows how to use the **translate** global configuration command to translate from an X.25 PAD to a LAT device on Network A. It is applied to Router-A. The configuration example includes an access list that limits remote LAT access through Router-A to connections from PAD-C. This example typifies the use of access lists in the Cisco IOS software. The first two lines define the scope of access-list 1. The first line specifies that access list 1 will permit all calls from X.121 address 44444. The caret symbol (^) specifies that the first number 4 is the beginning of the address number.The second line of the definition explicitly denies calls from any other number. (Refer to the appendix "Regular Expressions" in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2, for details concerning the use of special characters in defining X.121 addresses.)

```
! Define X25 access list to only allow pad-c.
x29 access-list 1 permit ^44444
x29 access-list 1 deny .*
!
! Set up translation.
translate x25 1111101 lat LAT-A access-class 1
```

The following example shows a simple X.25-to-TCP **translate x25** command. Packets coming in X.25 address 652365123 arrive via PVC 1 and are translated to TCP packets and sent out IP address 172.16.1.1.

```
translate x25 652365123 pvc 1 tcp 172.16.1.1
```

The following example shows a more complex configuration that calls an X.29 profile and swaps the default PAD operation of the router to that of an X.25 host. The name of the profile is fullpackets.

```
x29 profile fullpackets 2:0 3:0 4:100 7:21
translate x25 217536124 profile fullpackets tcp Host1 port 4006 swap
```

The following example shows the use of the X.25 incoming protocol **printer** keyword for an incoming X.25 connection:

```
translate x25 55555 printer tcp 172.16.1.1
```

The following examples causes the protocol translator to try connecting to IP address 172.16.1.1 and if that failed, to try IP address 172.16.2.1, and so on through all IP addresses listed in the **ip host** command:

```
ip host my-hosts 172.16.1.1 172.16.2.1 172.16.3.1
translate x25 55555 tcp my-hosts host-name
```

The following example uses the **rotor** keyword to cause the protocol translator to randomly choose one of the IP address listed in the **ip host** command and if it fails to connect, to try another IP address, until all are exhausted:

```
ip host my-hosts 172.16.1.1 172.16.2.1 172.16.3.1
translate x25 55555 tcp my-hosts host1 rotor
```

The following example translates X.25 packets to PPP. It enables routing updates between the two connections:

```
translate x25 12345678 ppp 10.0.0.2 routing
```

The following example permits clients running ARA to connect through the virtual terminal lines of the device to an AppleTalk network:

```
appletalk routing
translate x25 12345678 autocommand arap
  arap enable
  arap dedicated
  arap timelimit 45
  arap warningtime 5
  arap noguest
  arap require-manual-password
  arap net-access-list 614
```

The following example specifies IP pooling from a DHCP server named *D-Server1*. It then specifies that incoming TCP traffic be translated to SLIP. The DHCP server will dynamically assign IP addresses on the outgoing sessions.

```
ip address-pool dhcp-proxy-client
ip dhcp-server D-Server1
translate x25 5467835 ppp ip-pool scope-name D-Server1
```

The following example specifies a local IP pool named Pool2 with IP addresses ranging from 172.18.10.10 to 172.18.10.110. It then specifies that incoming X.25 traffic be translated to PPP. The local IP pool Pool2 will be used to dynamically assign IP addresses on the outgoing sessions.

```
ip-pool Pool2 172.18.10.10 172.18.10.110
translate x25 1234567 ppp ip-pool scope-name Pool2
```

The following example shows how to set the idle timer. X.25 calls are cleared if they are idle for the configured time.

```
translate x25 1234 idle 2 lat Service3
```


ECT nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 031
3698
Doc.

8022
A-

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 032
3698

translate x25 (virtual access interfaces)

When receiving an X.25 connection request to a particular destination address, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate x25** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate x25** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template. Table 49 lists all outgoing options and their corresponding interface configuration commands.

translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] **virtual-template** *number* [*global-options*]

no translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] **virtual-template** *number* [*global-options*]

Syntax Description

incoming-address	An X.25 and X.121 address that conform to specifications provided in the *CCITT 1984 Red Book.* This address generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.
incoming-options	(Optional) Incoming connection request keywords and arguments, as follows: • **accept-reverse**—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. This is an incoming option only. • **cud** *c-u-data*—Specifies the Call User Data (CUD) field to match in the X.25 Incoming Call packet. If not configured, the CUD in the Incoming Call packet must be blank. • **printer**—Supports LAT and TCP printing over an X.25 network among multiple sites. Provides an "interlock mechanism" between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. The **printer** keyword causes the protocol translation software to delay the call confirmation of an incoming X.25 call request until the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being confirmed and then cleared, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation.

- **profile** *profile*—Sets the X.3 PAD parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size*]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords and arguments to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are as follows: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.

virtual-template *number*	Applies the virtual interface template specified by the *number* argument in place of outgoing options.
global-options	(Optional) Translation options that can be used by any connection type and can be one or more of the following: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for X.25-to-TCP translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This keyword allows incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address or service name. The protocol connection information is followed by optional features for that connection, as appropriate. The global options, in general, apply to all the connection types, but there are exceptions. The **swap** keyword, for example, is for X.25- to-TCP translations only. See the example for more explanations on how to enter this command.

Rather than specifying outgoing translation options in the **translate** command, configure these options as interface configuration commands under the virtual interface template, then apply the virtual interface template to the **translate** command. Table 49 maps outgoing **translate** command options to interface commands you can configure in the virtual interface template.

Table 49 Mapping Outgoing translate x25 Options to Interface Commands

translate x25 Command Options	Corresponding Interface Configuration Command
ip-pool	**peer default ip address** {**ip-address** | **dhcp** | **pool** [*poolname*]}
header-compression	**ip tcp header compression** [**on** | **off** | **passive**]
routing	**ip routing** or **ipx routing**
mtu	**mtu**
keepalive	**keepalive**
authentication {**chap** | **pap**}	**ppp authentication** {**chap** | **pap**}
ppp use-tacacs	**ppp use-tacacs**
ipx loopback	**ipx ppp-client loopback** *number*

Examples

The following example shows a virtual template with PPP encapsulation specified by default (not explicit). It also specifies CHAP authentication and an X.29 access list.

```
x29 access-list 1 permit ^5555
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 172.16.2.129
 ppp authentication chap
!
translate x25 5555667 virtual-template 1 access-class 1
```

8618
A

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 036
Doc: 3698

transport input

To define which protocols to use to connect to a specific line of the router, use the **transport input** command in line configuration mode. To change or remove the protocol. use the **no** form of this command.

transport input {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

no transport input {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

Syntax Description

all	Selects all protocols.
lat	Selects the Digital LAT protocol and specifies both incoming reverse LAT and host-initiated connections.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Select NetWare Access Servers Interface (NASI) as the input transport protocol.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
pad	Selects X.3 packet assembler/disassembler (PAD) incoming connections.
rlogin	Selects the UNIX rlogin protocol.
telnet	Specifies all types of incoming TCP/IP connections.
v120	Selects the V.120 protocol for incoming asynchronous connections over ISDN.

Defaults

No protocols allowed on the line (**none**).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **none** keyword was added and became the default. Before Cisco IOS Release 11.1, the default keyword was **all**.

Usage Guidelines

Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You must specify an incoming transport protocol or specify the **transport input all** command before the line will accept incoming connections. For example, if you are using your router as a terminal server to make console-port connections to routers or other devices, you will not be able to use Telnet to connect to these devices. You will receive the message "Connection Refused." This behavior is new as of Cisco IOS software Release 11.1. Previous to Release 11.1, the default was the **transport input all** command, and the **all** keyword restored pre-Cisco IOS software Release 11.0 defaults. If you are upgrading to Cisco IOS software Release 11.1(1) or later releases from earlier Cisco IOS software Releases, you must configure the **transport input** {*protocol* | **all**} command, or you will be locked out of your router.

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space.

This command can be useful in distributing resources among different types of users, or in making certain that only specific hosts can access a particular port. When using two-step protocol translation, the **transport input** command is useful in controlling exactly which protocols can be translated to other protocols.

Access lists for each individual protocol can be defined in addition to the allowances created by the **transport input** command. Any settings made with the **transport input** command override settings made with the **transport preferred** command.

Examples

The following example sets the incoming protocol to Telnet for virtual terminal lines 0 to 32:

```
line vty 0 32
 transport input telnet
```

Related Commands

Command	Description
transport output	Determines the protocols that can be used for outgoing connections from a line.
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

038
Fls Nº
3698
Doc

transport output

To determine the protocols that can be used for outgoing connections from a line, use the **transport output** command in line configuration mode. To change or remove the protocol. use the **no** form of this command.

transport output {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

no transport output {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

Syntax Description

all	Selects all protocols.
lat	Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Selects NetWare Access Server Interface (NASI) as the output transport protocol.
none	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to **none**, the system no longer makes that assumption. No connection will be attempted if the command is not recognized.
pad	Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
rlogin	Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
telnet	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
v120	Selects the V.120 protocol for outgoing asynchronous connections over ISDN.

Defaults

Telnet

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords were added: • **all** • **lat** • **pad** • **rlogin** • **v120**

039
3698

Usage Guidelines

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space.

Any settings made with the **transport output** command override settings made with the **transport preferred** command.

Examples

The following example prevents any protocol selection:

```
transport output none
```

Related Commands

Command	Description
transport input	Defines which protocols to use to connect to a specific line of the router.
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

transport preferred

To specify the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection, use the **transport preferred** command in line configuration mode. To change or remove the protocol. use the **no** form of this command.

transport preferred {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

no transport preferred {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

Syntax Description

all	Selects all recognized protocols.
lat	Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Selects NetWare Access Server Interface (NASI) protocol.
none	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to **none**, the system no longer makes that assumption. No connection is attempted if the command is not recognized.
pad	Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
rlogin	Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
telnet	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
v120	Selects the asynchronous protocols over ISDN.

Defaults

Telnet

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords were added: • **lat** • **pad** • **rlogin**

8612
A.

Usage Guidelines

Specify the **transport preferred none** command to prevent errant connection attempts.

Any settings made with the **transport input** or **transport output** commands override settings made with the **transport preferred** command.

Examples

The following example sets the preferred protocol to Telnet on physical terminal line 1:

```
line tty 1
 transport preferred telnet
```

Related Commands

Command	Description
terminal transport preferred	Specifies the preferred protocol to use for the current session when a command does not specify one.
transport input	Defines which protocols to use to connect to a specific line of the router.
transport output	Determines the protocols that can be used for outgoing connections from a line.

RQS n° 03/2005 - CN
File N° 042
3698
Doc:

ttycap

To define characteristics of a terminal emulation file, use the **ttycap** command in global configuration mode. To delete any named ttycap entry from the configuration file, the **no** form of this command.

ttycap *ttycap-name termcap-entry*

no ttycap *ttycap-name*

Syntax Description

ttycap-name	Name of a file. It can be up to 32 characters long and must be unique.
termcap-entry	Commands that define the ttycap. Consists of two parts. (See the "Usage Guidelines" section for details.)

Defaults

VT100 terminal emulation

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use the **show ttycap** EXEC command to test for the availability of a ttycap.

Note Do not type a ttycap entry filename "default" or the Cisco IOS software will adopt the newly defined entry as the default.

The *termcap-entry* argument consists of two parts: a *name* portion and a *capabilities* portion.

The *name* portion is a series of names that can be used to refer to a specific terminal type. Generally, these names should represent commonly recognized terminal names (such as VT100 and VT200). Multiple names can be used. Each name is separated by a vertical bar symbol (|). The series is terminated by a colon symbol (:).

The following example illustrates a name specification for a VT100 termcap:

```
d0|vt100|vt100-am|vt100am|dec vt100:
```

The *capabilities* portion of the termcap entry consists of a sequence of termcap capabilities. These capabilities can include Boolean flags, string sequences, or numeric sequences. Each individual capability is terminated using a colon symbol (:). A *Boolean flag* can be set to true by including the two-character capability name in the termcap entry. The absence of any supported flag results in the flag being set to false.

The following is an example of a backspace Boolean flag:

```
bs:
```


FIS N° 043
Doc 3698

A *string sequence* is a two-character capability name followed by an equal sign (=) and the character sequence.

The following example illustrates the capability for homing the cursor:

```
ho=\E[H:
```

The sequence \E represents the ESC character.

Control characters can be represented in *string sequences* by entering a two-character sequence starting with a caret symbol (^), followed by the character to be used as a control character.

The following example illustrates the definition of a control character.

```
bc=^h.
```

In this example, the backspace is entered into the termcap entry as the string sequence as the characters "^h."

A *numeric sequence* is a two-character capability name followed by a number symbol (#) and the number.

The following example represents the number of columns on a screen.

```
co#80:
```

Use the backslash symbol (\ ) to extend the definition to multiple lines. The end of the ttycap termcap entry is specified by a colon terminating a line followed by an end-of-line character and no backslash.

For the definitions of supported Boolean-flag ttycap capabilities, see Table 50. For the definitions of supported string-sequence ttycap capabilities, see Table 51. For the definitions of supported number-sequence ttycap capabilities, see Table 52. For the definitions of supported color-sequence ttycap capabilities, see Table 53.

Table 50 Definitions of ttycap Capabilities: Boolean Flags

Boolean Flag	Description
am	Automatic margin
bs	Terminal can backspace with bs
ms	Safe to move in standout modes
nc	No currently working carriage return
xn	NEWLINE ignored after 80 columns (Concept)
xs	Standout not erased by overwriting (Hewlett-Packard)

Table 51 Definitions of ttycap Capabilities: String Sequences

String Sequence	Description
AL	Add line below with cursor sequence
bc	Backspace if not ^h
bt	Backtab sequence
ce	Clear to end of line
cl	Clear screen, cursor to upper left
cm	Move cursor to row number and column number

Table 51 Definitions of ttycap Capabilities: String Sequences (continued)

String Sequence	Description
cr	Carriage return sequence
cs	Change scrolling region
DL	Delete the line the cursor is on
ei	End insert mode
ho	Home, move cursor to upper left
ic	Character insert
im	Begin insert mode
is	Initialization string (typically tab stop initialization)
ll	Move cursor to lower left corner
md	Turn on bold (extra bright) character attribute
me	Turn off all character attributes
nd	Nondestructive space
nl	Newline sequence
pc	Pad character if not NULL
rc	Restore cursor position
rs	Resets terminal to known starting state
sc	Save cursor position
se	End standout mode (highlight)
so	Start standout mode (highlight)
ta	Tab
te	End programs that use cursor motion
ti	Initialization for programs that use cursor motion
uc	Underline character at cursor
ue	End underline mode
up	Move cursor up
us	Begin underline mode
vb	Visual bell
vs	Visual cursor
ve	Normal cursor

CPMI - CORREIOS
045
3698

Table 52 Definitions of ttycap Capabilities: Number Sequences

Number Sequence	Description
li	Lines on the screen
co	Columns on the screen
sg	Standout glitch, number of spaces printed when entering or leaving standout display mode
ug	Underline glitch, number of spaces printed when entering or leaving underline mode

Table 53 Definitions of ttycap Capabilities: Color Sequences

Color Sequence	Description
x0	Black
x1	Blue
x2	Red or orange
x3	Pink or purple
x4	Green, which is the default color
x5	Turquoise
x6	Yellow
x7	Gray or white

The ttycap database uses these color sequences to translate IBM directives into screen drawing commands. These color sequences control only foreground terminal colors. They do not control background color, which is configured to black by default.

Examples

The following is an example of a ttycap file. Refer to the chapter "Configuring Dial-In Terminal Services" in the *Cisco IOS Terminal Services Configuration Guide* and the tn3270.examples file in the Cisco ftp@cisco.com directory for more examples.

```
ttycap ttycap1\
d0|vt100|vt100-am|vt100am|dec vt100:do=^J:co#80:li#24:\
cl=50^[[;H^[[2J:bs:am:cm=5^[[%i%d;%dH:nd=2^[[C:up=2^[[A:\
ce=3^[[K:so=2^[[7m:se=2^[[m:us=2^[[4m:ue=2^[[m:md=2^[[1m:\
me=2^[[m:ho=^[[H:xn:sc=^[7:rc=^[8:cs=^[[%i%d;%dr:
```

Related Commands

Command	Description
keymap-type	Specifies the keyboard map for a terminal connected to the line.
terminal-type	Specifies the type of terminal connected to a line.

txspeed

To set the terminal transmit speed (how fast the terminal sends information to the modem), use the **txspeed** command in line configuration mode. To return to the default setting, use the **no** form of this command.

txspeed *bps*

no txspeed

Syntax Description

bps	Baud rate, in bits per second (bps).

Defaults

9600 bps

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the router. The Cisco IOS software will indicate if the speed you select is not supported.

Examples

The following example sets the transmit speed for line 5 to 2400 bps:

```
line 5
 txspeed 2400
```

Related Commands

Command	Description
rotary-group	Sets the terminal receive speed (how fast the terminal receives information from the modem).
source template	Sets the flow control start character.
terminal txspeed	Sets the terminal transmit speed (how fast the terminal can send information) on the current line and session.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls nº 047
3698

where

To list the open sessions, use the **where** command in EXEC mode.

where

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.

Usage Guidelines

The **where** command displays all open sessions associated with the current terminal line.

The **Ctrl^x**, **where**, and **resume** commands are available with all supported connection protocols.

Examples

The following is sample output from the **where** command:

```
Router# where

Conn Host                Address          Byte    Idle  Conn Name
   1 MATHOM              192.168.7.21        0       0  MATHOM
*  2 CHAFF               172.18.12.19        0       0  CHAFF
```

The asterisk (*) indicates the current terminal session.

Table 54 describes the significant fields shown in the display.

Table 54 where Field Descriptions

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes for the user to see on the connection.
Idle	Interval, in minutes, since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands

Command	Description
show sessions	Displays information about open LAT, Telnet, or rlogin connections.

x25 subaddress

To append either a physical port number or a value specified for a line as a subaddress to the X.121 calling address, use the **x25 subaddress** command in line configuration mode. To disable subaddressing, the **no** form of this command.

x25 subaddress {**line** | *number*}

no x25 subaddress {**line** | *number*}

Syntax Description

line	Physical port number for the indicated line to be appended to the X.121 address as the subaddress.
number	Numeric variable assigned to a specific line.

Defaults

No default behavior or values.

Command Modes

Line configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **x25 subaddress line** command to create a unique X.121 calling address by adding either a physical port number or a numeric value for a line as a subaddress to the X.121 calling address.

Examples

The following example shows how to configure subaddressing on virtual terminal lines 10 through 20 by appending the line number as a subaddress to the X.121 calling address:

```
line vty 10 20
x25 subaddress line
```

The following example shows how to configure subaddressing on the first five TTY lines by appending the value 09 as a subaddress to the X.121 calling address of an X.28 connection originating on these lines:

```
line 1 5
x25 subaddress 9
autocommand x28
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.

x28

To enter X.28 mode and access an X.25 network or set X.3 packet assembler/disassembler (PAD) parameters, use the **x28** command in EXEC mode. To exit X.28 mode, use the **no** form of this command.

x28 [escape *character-string*] **[noescape] [nuicud] [profile** *file-name*] **[reverse] [verbose]**

no x28 [escape *character-string*] **[noescape] [nuicud] [profile** *file-name*] **[reverse] [verbose]**

Syntax Description

escape *character-string*	(Optional) Specifies a character string to use to exit X.28 mode and return to EXEC mode. The character string can be any string of alphanumeric characters. The Ctrl key can be used in conjunction with the character string.
noescape	(Optional) Specifies that no escape character string is defined (user cannot return to EXEC mode). On the console line, the **noescape** option is ignored, and the default escape sequence is used (**exit** command).
nuicud	(Optional) Specifies the network user identification (NUI) data to not be placed in the NUI facility of the call request. Instead the data is placed in the Call User Data (CUD) area of the call request packet.
profile *file-name*	(Optional) Specifies using a user-configured profile of X.3 parameters. A profile is created with the **x29 profile** EXEC command.
reverse	(Optional) Specifies reverse charges for outgoing calls made from the local router to the destination device.
verbose	(Optional) Displays optional service signals such as the called DTE address, facility block, and CUD.

Defaults

Disabled. X.28 mode uses standard X.28 command syntax.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If both the **escape** and **noescape** options are not set, the default escape sequence is used (**exit** command).

X.28 mode is identified with an asterisk (*) router prompt. After you enter this mode, the standard X.28 user interface (with the exception of the escape sequence) is available. From this interface, you can configure a PAD device using X.3 parameters, or you can access an X.25 network.

In X.28 mode, you can set PAD command signals using standard or extended command syntax. For example, you can enter the **clr** command or **clear** command to clear a virtual call. A command specified with standard command syntax is merely an abbreviated version of the extended syntax version.

Table 55 lists the commands available in both standard and extended command syntax.

Table 55 Available PAD Command Signals

Standard Syntax	Extended Syntax	Description
break		Simulate an asynchronous break.
call		Place a virtual call to a remote device.
clr	**clear**	Clear a virtual call.
command-signal[1]		Specifies a call request without using a standard X.28 command, which is entered with the following syntax: *facilities-x121-address***D***call-user-data*.
help		Display help information. (See Table 57.)
iclr	**iclear**	Request the remote device to clear the call.
int	**interrupt**	Send an Interrupt Packet.
par? **par**	**parameter** **read**	Display the current values of local parameters. (See Table 56.)
prof	**profile** *file-name*	Load a standard or a named profile.
reset		Reset the call.
rpar?	**rread**	Display the current values of remote parameters.
rset?	**rsetread**	Set and then read the values of remote parameters.
set		Change the values of local parameters. (See Table 56.)
set?	**setread**	Change and then read the values of parameters.
stat	**status**	Request the status of a connection.
selection pad		Set up a virtual call.

1. This is an example of issuing a call request command: the **R,G23,P2-234234Duser1** command.

Table 56 lists the different types of parameters you can set using the **set** *parameter-number*:*new-value* PAD command signal from X.28 mode. Refer to the "X.3 PAD Parameters" appendix in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2 for more complete information about these parameters. See Table 35 in this publication for a list of ASCII characters.

Table 56 Supported X.3 PAD Parameters

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
1	PAD recall using a character	Minimum value: 0; maximum value: 126; X.28 PAD user emulation mode default: 1. **Note** Not supported by PAD EXEC user interface.
2	Echo	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode defaults: 1.
3	Selection of data forwarding character	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 2 (CR); X.28 PAD user emulation mode default: 126 (~).

Table 56 Supported X.3 PAD Parameters (continued)

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
4	Selection of idle timer delay	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 1; X.28 PAD user emulation mode default: 0.
5	Ancillary device control	Minimum value: 0; maximum value: 2; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
6	Control of PAD service signals	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. **Note** Not supported by PAD EXEC user interface.
7	Action upon receipt of a BREAK signal	Minimum value: 0; maximum value: 31; PAD EXEC mode default: 4; X.28 PAD user emulation mode default: 2.
8	Discard output	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
9	Padding after Return	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
10	Line folding	Not supported.
11	DTE speed (binary speed of start-stop mode DTE)	Minimum value: 0; maximum value: 18; PAD EXEC mode and X.28 PAD user emulation mode default: 14.
12	Flow control of the PAD by the start-stop DTE	Minimum value: 0; maximum value: 1; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
13	Line feed insertion (after a Return)	Minimum value: 0; maximum value: 7; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
14	Line feed padding	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
15	Editing	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
16	Character delete	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 127 (DEL).
17	Line delete	Minimum value: 0; maximum value: 127; PAD EXEC mode default: 21 (Ctrl-U); X.28 PAD user emulation mode default: 24 (Ctrl-X).
18	Line display	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 18 (Ctrl-R).
19	Editing PAD service signals	Minimum value: 0; maximum value: 126; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. **Note** Not supported by PAD EXEC user interface.

CPMI – CORREIO
Fls nº 052
3698

Table 56 Supported X.3 PAD Parameters (continued)

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
20	Echo mask	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0. **Note** Not supported by PAD EXEC user interface.
21	Parity treatment	Minimum value: 0; maximum value: 4; PAD EXEC mode and X.28 PAD user emulation mode default: 0. **Note** For additional values that can be selected for parameter 21 and to select parity treatment to conform to the French Transpac public switched data network and its technical specification and utilization of networks standards (STUR), refer to the appendix "X.3 PAD Parameters" in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2.
22	Page wait	Not supported.

Note Abbreviated X.121 addresses are not supported. Such addresses start with a period, are alphanumeric, and are mapped to a full X.121 address by the PAD.

Table 57 lists the options for the X.28 **help** command.

Table 57 X.28 help Options

Command	Description
help	Describes the **help** PAD command.
help command	Displays the list of available PAD command signals.
help parameter	Displays the list of available X.3 PAD parameters.
help parameter *number*	Displays the specified X.3 PAD parameter and its current value.
help list	Lists the available help subjects.
help profiles	Lists available profiles.
help profile *name*	Displays the specified parameter name and current value.
help *any-PAD-command*	Describes the specified PAD command signal.

You can issue call requests from X.28 mode without using standard X.28 commands by using the following command syntax:

*facilities-x121-address***D***call-user-data*

where:

facilities	Applies X.25 facilities to the outgoing call. The hyphen is mandatory.
x121-address	Specifies the address of the remote X.25 device.
D	Facility request code that specifies CUD for the outgoing call.
call-user-data	Specifies the data that accompanies the call request packet sent to the remote X.25 device.

The following rules apply to all call requests parsed in X.28 mode:

- When an X.121 address specified using standard command syntax is followed by an optional CUD field, the call is placed to the X.121 address.
- When standard command syntax is used, one or more facility request codes can be entered, followed by the code value. Additional facility request codes and values also can be entered. Separate each entry with a comma, followed by a dash. An X.121 address and optional CUD can follow this entry.
- If an X.28 command is not entered, a call request is assumed.
- Ensure that the call request begins with a facility code letter, and that it contains a hyphen (-) followed by a string of digits (the X.121 address). The call request can be terminated by an asterisk (*), a "P," or a "D," followed by some data.
- When using extended command syntax is used, the **call** command uses the facility codes and X.121 address as its operand.
- If facility codes are entered without an X.121 address, remember the codes for the next call. When a call is completed, forget the facility codes until they are once again set.

Table 58 shows examples of parsed call requests.

Table 58 Example X.28 Call Requests

Command	Description
123456789	Calls this X.121 address.
123456789*userdata	Calls this X.121 address, with specified data.
123456789Puserdata	Calls this X.121 address, with specified data.
123456789Duserdata	Calls this X.121 address, with specified data.
Nabcd-123456789	Calls this X.121 address, with NUI set to abcd.
Nabcd,R-123456789	Calls 123456789 with NUI of abcd, and with reverse charging.

Examples

The following example uses the ? command to display the optional X.28 keywords:

```
Router# x28 ?

  debug     Turn on Debug Messages for X28 Mode
  escape    Set the string to escape from X28 PAD mode
  noescape  Never exit x28 mode (use with caution)
  nuicud    All calls with NUI, are normal charge with the NUI placed in Call
            User Data
```

```
profile   Use a defined X.3 Profile
reverse   All calls default to reverse charge
verbose   Turn on Verbose Messages for X28 Mode
<cr>
```

After you are in X.28 mode, use the **call** PAD signal command to place a virtual call:

```
Router# x28

* call 123456
```

The following example enters X.28 mode with the **x28** EXEC command and configures a PAD with the **set** X.3 parameter command. The **set** command sets the idle time delay to 40 seconds.

```
Router# x28

* set 4:40
```

Related Commands

Command	Description
pad	Logs in to a PAD.

ECT nº 03/2002 - CN - CPMI - CORREIOS
Fls Nº 055
Doc 3698

8598
x3
A

x3

To set X.3 packet assembler/disassembler (PAD) parameters, use the **x3** command in EXEC mode.

x3 *parameter*:*value*

Syntax Description

parameter:*value*	Sets the PAD parameters. (See Table 56 in the **x28** command description.)

Defaults

For outgoing connections, the X.3 parameters default to the following:

```
2:1, 3:2, 4:1, 7:4, 16:127, 17:21, 18:19
```

All other parameters default to zero, but can be changed using the **/set** switch keyword with either the **resume** command or the **x3** command.

For incoming PAD connections, the software sends an X.29 SET PARAMETER packet to set only the following parameters:

```
2:0, 4:1, 7:21, 15:0
```

For a complete description of the X.3 PAD parameters, see the appendix titled "X.3 PAD Parameters" in the *Cisco IOS Terminal Services Configuration Guide*.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You can have several PAD connections open at the same time and switch between them. You can also exit a connection and return to the user EXEC prompt at any point.

To open a new connection, first suspend the current connection by pressing the escape sequence (**Ctrl-Shift-6** then **x** [**Ctrl^x**] by default) to return to the system command prompt, then open the new connection with the **pad** command.

You can have several concurrent sessions open and switch between them. The number of PAD sessions that can be open is defined by the **session-limit** command.

To switch between sessions you must escape one session and resume a previously opened session. Use the Ctrl^x sequence to escape out of a connection, use the **where** EXEC command to check the connection number, and then use the **resume** command with the connection number to resume the suspended connection. These commands are available with all supported connection protocols.

You can issue any of the following commands to terminate a terminal session:

- **exit**
- **quit**
- **logout**

056
3698

8597
A.

To display information about packet transmission and X.3 PAD parameter settings, use the **show x25 pad** command.

Examples

The following example shows how to change a local X.3 PAD parameter from a remote X.25 host using X.29 messages, which is a secure way to enable a remote host to gain control of local PAD. The local device is named Router-A. The remote host is named Router-B. The parameters listed in the ParamsIn field are incoming parameters, which are sent by the remote PAD. The parameters listed in the ParamsOut field are parameters sent by the local PAD.

```
Router-A# pad 123456
Trying 123456...Open

Router-B> x3 2:0
Router-B>
Router-A# show x25 pad

tty0, connection 1 to host 123456

Total input: 12, control 3, bytes 35. Queued: 0 of 7 (0 bytes).
Total output: 10, control 3, bytes 64.
Flags: 1,   State: 3,   Last error: 1
 ParamsIn:  1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0,
    8:0, 9:0, 10:0, 11:0, 12:0, 13:0, 14:0, 15:0,
    16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0,
 ParamsOut:  1:1, 2:0, 3:2, 4:1, 5:1, 6:0, 7:21,
    8:0, 9:1, 10:0, 11:14, 12:1, 13:0, 14:0, 15:0,
    16:127, 17:21, 18:18, 19:0, 20:0, 21:0, 22:0,
Router-A#
```

Related Commands

Command	Description
resume (X.3 PAD)	Sets X.3 parameters for PAD connections.

RGS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 057
3698
Doc

xremote

To prepare the router for manual startup and initiate an XRemote connection, use the **xremote** command in EXEC mode. This command begins the instructions that prompt you through the connection.

xremote

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

If you do not use a host computer that supports XDMCP or LAT, you must use manual session startup. Manual session startup involves the following steps:

Step 1 Enable XRemote manually on the router port.

Step 2 Connect to the host computer by using a **telnet**, **lat**, or **rlogin** command, then log in as usual.

Step 3 Set the location of the X display.

Step 4 Start client applications.

Step 5 Return to the EXEC prompt.

Step 6 Enter the **xremote** command to enable XRemote manually again on the server port.

Note In manual operation, the server and X terminal remain in XRemote mode until all clients disconnect or the access server receives a reset request from the X terminal. A session might terminate during startup because you invoked transient X clients that set some parameters (such as **xset** or **xmodmap**) and then disconnected. One session must always be open or the connection resets.

Refer to the *Cisco IOS Terminal Services Configuration Guide* for more information about how to establish XRemote sessions between servers.

Examples

The following example starts a manual XRemote session:

```
dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again
```

The router replies with a message informing you of your X display location. Use this information to tell the XRemote host the location of your X display server. If no clients are found, you see the following message:

```
No X clients waiting - check that your display is darkstar:2006
```

The following example shows a connection from an X display terminal through a router to a host running client programs:

```
dialup> xremote

XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again

dialup> telnet eureka
Trying EUREKA.NOWHERE.COM (722.18.1.55)... Open

SunOS UNIX (eureka)

login: deal
Password:

Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994

eureka% setenv DISPLAY dialup:2006
eureka% xterm &
[1] 15439

eureka% logout

[Connection to EUREKA closed by foreign host]

dialup> xremote
Entering XRemote
```

The following procedure shows how an XRemote connection is established for a configuration like the one shown in Figure 2. This example assumes that the administrator has set the display environment variable for the user to identify the X display terminal.

Step 1 From the PCX, MacX, or UNIX machine in Figure 2, the user connects to port 9003 on access server 1. If your administrator has configured a rotary number 7, the user connects to port 10007. For more information about rotary groups, refer to the *Cisco IOS Dial Technologies Configuration Guide*.

Step 2 Access server 1 connects the user to a modem.

Step 3 The modem calls access server 2.

Step 4 The user enters **xremote** at the access server 2 prompt.

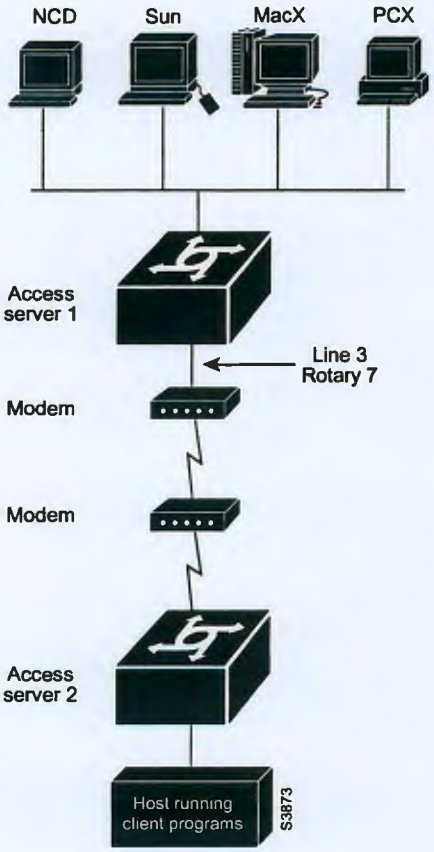
Step 5 The user connects to the host from access server 2 using the **telnet** command.

Step 6 The user starts the X client program that will run on the host and display on the X display server (PCX, MacX, or UNIX host).

Step 7 The user escapes from the host back to the AccessServer2, or logs out if clients were run in the background, and enters the **xremote** command at the AccessServer2 prompt.

You can use the master indexes or search online to find documentation of related commands.

Figure 2 XRemote Session Between Servers



The following example shows how to make an XRemote connection between servers. The number 9016 in the first line of the display indicates a connection to individual line 16. If the administrator had configured a rotary connection, the user would enter 10000 plus the number of the rotary instead of 9016.

```
Router% telnet golden-road 9016

Trying 192.168.7.84 ...
Connected to golden-road.cisco.com.
Escape character is '^]'.

User Access Verification

Password:
Password OK
```

```
 --- Outbound XRemote service ---
Enter X server name or IP address: innerspace
Enter display number [0]:

 Connecting to tty16... please start up XRemote on the remote system

atdt 13125554141
DIALING
RING
CONNECT 14400

User Access Verification
Username: deal
Password:
  Welcome to the cisco dial-up access server.

dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again

dialup> telnet sparks
Trying SPARKS.NOWHERE.COM (172.18.1.55)... Open

SunOS UNIX (sparks)

login: deal
Password:
Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994

sparks% setenv DISPLAY dialup:2006
sparks% xterm &
[1] 15439

sparks% logout

[Connection to SPARKS closed by foreign host]

dialup> xremote
Entering XRemote
```

Related Commands

Command	Description
xremote lat	Initiates a DECwindow session over a LAT connection.
xremote xdm	Activates automatic session startup for an XRemote connection.

xremote lat

To initiate a DECwindow session over a local-area transport (LAT) connection, use the **xremote lat** command in EXEC mode.

xremote lat *service*

Syntax Description

service	Name of the desired LAT service.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If your host computer supports DECwindows login sessions, you can use automatic session startup to make an XRemote session connection. Once the system administrator at the remote host configures support for DECwindows over LAT, use the **xremote lat** EXEC command to initiate the connection. After you issue this command, the following events occur:

- The XRemote font server down-line loads several initial fonts for the DECwindows login display.
- The terminal displays the DIGITAL logo and DECwindows login box.

Log in to the host. Upon completion of login, more fonts are loaded, and the remote session begins.

Note Because of heavy font usage, DECwindows applications can take longer than expected to start when XRemote is used. Once the application starts, performance and access times should be as expected.

To exit XRemote sessions, you must quit all active X connections, usually with a command supported by your X client system. Usually when you quit the last connection (when all client processes are stopped), XRemote closes and you return to the EXEC prompt. However, your X client system determines how the session closes.

Examples

The following example begins connection with a LAT service named service1:

```
xremote lat service1
```

Related Commands

Command	Description
xremote	Prepares the router for manual startup and initiates an XRemote connection.
xremote xdm	Activates automatic session startup for an XRemote connection.

8591
A-

xremote tftp buffersize

To change the buffer size used for loading font files, use the **xremote tftp buffersize** command in global configuration mode. To restore the buffer size to the default value, use the **no** form of this command.

xremote tftp buffersize *buffersize*

no xremote tftp buffersize

Syntax Description

buffersize	Buffer size in bytes. This is a decimal number in the range from 4096 to 70000 bytes. The default is 70000.

Defaults

70000 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the X terminal requests that a font file be loaded, the Cisco IOS software must first load the font file into an internal buffer before passing it to the X terminal. The default value of 70000 bytes is adequate for most font files, but the size can be increased as necessary for nonstandard font files.

The buffer size can be set as low as 4096 bytes and as large as the available memory on the router will allow. If you are using local-area transport (LAT) font access, you should not lower the buffer size below the default, because the font directory for all of the LAT fonts (created internally) requires 70000 bytes.

This command applies to both TFTP and LAT font access.

Examples

The following example sets the buffer size to 20000 bytes:

```
xremote tftp buffersize 20000
```


ROS nº 03/2005 - CN -
CPMI - CORREIOS
063
Fls. Nº
3698
Doc.

8590
A·

xremote tftp host

To add a specific Trivial File Transfer Protocol (TFTP) font server as a source of fonts for the terminal, use the **xremote tftp host** command in global configuration mode. To remove a font server from the list, use the **no** form of this command.

xremote tftp host *host-name*

no xremote tftp host *host-name*

Syntax Description

host-name	IP address or name of the host containing fonts.

Defaults

No TFTP font server is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Each time a new host name is entered, the list in the Cisco IOS software is updated. Font servers are queried in the order of their definition when the X terminal requests a font.

Examples

The following example sets the host named IBM-1 as an XRemote TFTP font server:

```
xremote tftp host IBM-1
```

The following example sets the host with IP address 10.0.0.7 as an XRemote TFTP font server:

```
xremote tftp host 10.0.0.7
```


ROS n° 03/2005 - CN
CPM - ECT
File N° 064
3698
Doc

xremote tftp retries

To specify the number of retries the font loader will attempt before declaring an error condition, use the **xremote tftp retries** command in global configuration mode. To restore the default retries number, use the **no** form of this command.

xremote tftp retries *retries*

no xremote tftp retries

Syntax Description

retries	(Optional) Number of retries. Acceptable values are decimal numbers in the range from 1 to 15.

Defaults

3 retries

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Under certain conditions, you might need to increase the number of retries, particularly if the font servers are known to be heavily loaded.

Examples

The following example sets the number of font loader retries to 5:

```
xremote tftp retries 5
```

xremote xdm

To activate automatic session startup for an XRemote connection, use the **xremote xdm** command in EXEC mode.

xremote xdm [*host-name*]

Syntax Description

host-name	(Optional) Host computer name or IP address.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If your host computer supports a server running X Display Manager Control Protocol (XDMCP) (such as the xdm program included in X11R4 or later), you can use automatic session startup to make an XRemote session connection using the **xremote xdm** EXEC command.

This command sends an XDMCP session startup request to the host computer. If you do not specify a host name or IP address, a broadcast message is sent to all hosts. The first host to respond by starting up a session is used.

The XRemote (the host) server and X terminal stay in XRemote mode until either the display manager terminates the session or the XRemote server receives a reset request from the X terminal.

To exit XRemote sessions, you must quit all active X connections, usually with a command supported by your X client system. Usually when you quit the last connection (all client processes are stopped), XRemote closes and you return to the EXEC prompt. However, your remote X client system determines how the session closes.

To terminate a session, disconnect from the device on the network using the command specific to that device. Then exit from the EXEC by using the **exit** command.

Examples

The following example starts a session with a remote host named host1:

```
xremote xdm host1
```

Related Commands

Command	Description
xremote	Prepares the router for manual startup and initiates an XRemote connection.
xremote lat	Initiates a DECwindow session over a LAT connection.

8587
A

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 067
3698

RQS nº 03/2005 - CN -
CPMI - CORREIOS
068
Fls. Nº
3698
Doc.

8586
A.

Cisco VPN 3000 Concentrator Series

Product Overview

The Cisco VPN 3000 Concentrator Series is a best-of-breed, remote-access VPN solution for enterprise-class deployment. A standards-based, easy-to-use VPN client and scalable VPN tunnel termination devices are included as well as a management system that enables corporations to easily install, configure and monitor their remote access VPNs. Incorporating the most-advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications. Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP) modules, enable users to easily add capacity and throughput. The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, VPN 3002 Hardware Client, the Microsoft Windows 2000 L2TP/IPsec Client and the Microsoft PPTP for Windows 95, Windows 98, Windows NT, and Windows 2000.

The Cisco VPN 3000 Concentrator is available in five different models to support any business:

Cisco VPN 3005 Concentrator

The 3005 is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4Mbps maximum performance) and up to 100 simultaneous sessions. Encryption processing is performed in software. The 3005 does not have built-in upgrade capability.

Cisco VPN 3015 Concentrator

The 3015 is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-x T1/E1 (4Mbps maximum performance) and up to 100 simultaneous sessions. Like the 3005, encryption processing is performed in software, but the 3015 is also field-upgradeable to models 3030, 3060, and 3080.

Cisco VPN 3030 Concentrator

The 3030 is a VPN platform designed for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through fractional T3 (50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The 3030 is field-upgradeable to the 3060. Redundant and non-redundant configurations are available.

Cisco VPN 3060 Concentrator

The 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and non-redundant configurations are available.

Cisco VPN 3080 Concentrator

The 3080 is optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous remote access sessions. Specialized SEP modules perform hardware-based acceleration. The VPN 3080 is available in a fully redundant configuration only.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to compliant* Cisco Remote Access VPN devices. This thin design, IPSec-compliant implementation is available via CCO download for use with any compliant* Cisco Remote Access VPN product and is included free of charge with the Cisco VPN 3000 Concentrator. The client can be pre-configured for mass deployments and initial logins require very little user intervention.

069
3698

—Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.

—Firewall capabilities through stateless packet filtering and address translation to assure the required security of a corporate LAN.

—User and group level management offers maximum flexibility.

- High Availability

—Redundant subsystems and multi-chassis fail-over capabilities ensure maximum system uptime.

—Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

- Robust Management

—The Cisco VPN 3000 Concentrators can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, Secure Telnet, SSH, and via a console port.

—Configuration and monitoring capability is provided for both the enterprise and the service provider.

—Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies.

Specifications

Hardware

Table 19-7: Technical Specifications for Cisco VPN 3000 Series

Description	Specification
Processor	Motorola PowerPC Processor
Ports	Console port-Asynchronous serial (DB-9)
Memory	Redundant system images (Flash) Variable memory options (see chart)
Encryption	3005, 3015: Software encryption 3030, 3060, 3080: Hardware encryption
Embedded LAN Interfaces	3005: Two auto-sensing, full-duplex 10/100BaseTX Fast Ethernet (public/untrusted, private/trusted) 3015- 3080: Three auto-sensing, full-duplex 10/100BaseTX Fast Ethernet (public/untrusted, private/trusted and DMZ)
Instrumentation	3005 Front panel: Unit status indicator 3005 Rear panel: Status light-emitting diodes (LED) for Ethernet ports 3015-3080 Front panel: Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan 3015-3080 Rear panel: Status LEDs for Ethernet modules, expansion modules, power supplies 3015-3080:Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Table 19-8: Power Requirements for Cisco VPN 3000 Series

Description	3005	3015 - 3080
Nominal	15 watts (51.22BTU/hr)	35 watts (119.50BTU/hr)
Maximum	25 watts (85.36BTU/hr)	50 watts (170.72BTU/hr)
Input Voltage	100-240VAC	100-240VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

RCS nº 070
3698

Description		Specification
Management	Configuration	Embedded management interface is accessible via console port, Telnet, SSH, and Secure HTTP
		Administrator access is configurable for five levels of authorization. Authentication can be performed externally via TACACS+
		Role-based management policy separates functions for service provider and end-user management
	Monitoring	Event logging and notification via e-mail (SMTP)
		Automatic FTP backup of event logs
		SNMP MIB-II support
		Configurable SNMP traps
		Syslog output
		System status
		Session data
		General statistics
Security	Authentication and Accounting Servers	Support for redundant external authentication servers:
		- RADIUS (Remote Authentication Dial-In User Service)
		- Microsoft NT Domain authentication
		- RSA Security Dynamics (SecurID Ready)
		Internal Authentication server for up to 100 users
		TACACS+ Administrative user authentication
		X.509v3 Digital Certificates
		RADIUS accounting
	Internet-Based Packet Filtering	Source and destination IP address
		Port and protocol type
		Fragment protection
		FTP session filtering
	Policy Management	By individual user or group
		- Filter profiles
		- Idle and maximum session timeouts
		- Time and day access control
		- Tunneling protocol and security authorization profiles
		-IP Pool
		Authentication Servers

Ordering Information

Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at

http://www.cisco.com/cgi-bin/order/pricing_root.pl

071

3698

8581
A

RGS nº 03/2005 - CN -
CPMI - CORREIOS
072
Fls Nº
3698
Doc:

8583 A

Table 19-9: Physical and Environmental Characteristics for Cisco VPN 3000 Series

Description	3005	3015	3030	3060	3080
Dimensions (HxWxD)	1.75 x 17.5 x 11.5 in. (4.45 x 44.45 x 29.21 cm)	3.5 x 17.5 x 14.5 in. (8.89 x 44.45 x 36.83 cm)	Same as 3015	Same as 3015	Same as 3015
Weight	8.5 lbs (3.9 kg)	27 lbs (12.3 kg)	28 lbs (12.7 kg)	33 lbs (15 kg)	33 lbs (15 kg)
Operating Temperature	32 to 131°F (0 to 55°C)	Same as 3005	Same as 3005	Same as 3005	Same as 3005
Storage Temperature	-4 to 176°F (-20 to 80°C)	Same as 3005	Same as 3005	Same as 3005	Same as 3005
Humidity	0-to-95% non-condensing	Same as 3005	Same as 3005	Same as 3005	Same as 3005

Table 19-10: Regulatory Approvals for Cisco VPN 3000 Series

Description	Specification
Regulatory Compliance	CE Marking
Safety	UL 1950, CSA
EMC	FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN 50082-1, AS/NZS 3548 Class A, VCCI Class A

Software

Table 19-11: Software Requirements for Cisco VPN 3000 Series

Description		Specification
Compatibility	Client Software Compatibility	Cisco VPN Client (IPsec) for Windows 95, 98, ME, NT 4.0 and Windows 2000, including centralized split-tunneling control and data compression
		Cisco VPN 3002 Hardware Client
		Microsoft PPTP/MPPE/MPPC
		Microsoft L2TP/IPsec for Windows 2000
		MovianVPN (Certicom) Handheld VPN Client with ECC
	Tunneling Protocols	IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec
	Encryption/ Authentication	IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) with MD5 or SHA, MPPE using 40/128-bit RC4
	Key Management	Internet Key Exchange (IKE)
	Routing Protocols	RIP, RIP2, OSPF, Static, Automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
	Third-Party Compatibility	Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Mac and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, GTE Cybertrust, Baltimore, RSA Keon, Verisign
	High Availability	VRRP protocol for multi-chassis redundancy and fail-over
		Destination pooling for client-based fail-over and connection re-establishment
		Redundant SEP modules (optional), power supplies, and fans (3015 - 3060)
		Redundant SEP modules, power supplies, and fans (3080)

073
3698

VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management. The Cisco VPN client provides support for Windows 95, 98, ME, NT 4.0, and 2000.

The Cisco VPN Client is compatible with the following Cisco product versions (compliant Cisco Remote Access products):

- Cisco VPN 3000 Concentrator Release 3.0
- IOS-based platforms (future availability)
- Cisco VPN 5000 Concentrator Release 6.2 and greater (future availability)
- PIX Firewalls Release 6.0 and greater (future availability)

Key Features and Benefits

Cisco VPN 3000 Concentrator Series Features

Table 19-6: Feature Summary for the Cisco VPN 3000 Series

Feature	Cisco 3005	Cisco 3015	Cisco 3030	Cisco 3060	Cisco 3080
Simultaneous Users	100	100	1500	5000	10000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	N/A	N/A	Option	Option	Yes
Available Expansion Slots	0	4	3	2	N/A
Upgrade Capability	No	Yes	Yes	N/A	N/A
System Memory	32 MB (fixed)	64 MB	128 MB	256 MB	256 MB
T1 WAN Module	Fixed option	Option	Option	Option	Option
Hardware	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

The Cisco VPN 3000 Concentrator Series supports the entire range of enterprise applications.

Product Highlights

- High-Performance, Distributed-Processing Architecture
  - —Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (3030 - 3080).
  - —Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPSec connections.
- Scalability (3015-3080)
  - —Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
  - —System architecture is designed to supply consistent, high-availability performance.
  - —All digital design provides the highest reliability and 24-hour continuous operation.
  - —Robust instrumentation package provides run-time monitoring and alerts.
  - —Microsoft compatibility offers large-scale client deployment and seamless integration with related systems.
- Security

ROS nº 032666 - CN -
CPMI - CORREIOS
Fls Nº 075
Doc: 3698

Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.0

CCO Date: April 7, 2003

Part Number 78-15416-01

Introduction

Note You can find the most current documentation for released Cisco VPN 3000 products at http://www.cisco.com or http://cco.cisco.com. These electronic documents might contain updates and changes made after the hard-copy documents were printed.

These release notes are for Cisco VPN 3000 Series Concentrator Release 4.0 software. These release notes describe new features, limitations and restrictions, interoperability notes, and related documentation. They also list issues you should be aware of and the procedures you should follow before loading this release. The

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Platform Files

Release 4.0 contains two binary files, one for each of two platforms:

- Files beginning with `vpn3000-` support the VPN Concentrator 3015 through 3080 platforms.
- Files beginning with `vpn3005-` support the VPN Concentrator 3005 platform only.

Caution Be sure you install the correct file for the platform you are upgrading.

Upgrading to Release 4.0

This section contains information about upgrading from earlier releases to Release 4.0.

When upgrading VPN 3000 Concentrator releases, you must clear the cache in your browser to ensure that all new screens display correctly when you are managing the VPN Concentrator.

Note You must also log in and click "Save Needed" to add new Release 4.0 parameters to the configuration file. These new Release 4.0 parameters are added to the running configuration immediately, but they are not added to the saved configuration until you click the "Save Needed" or "Save" icon in the VPN Concentrator Manager.

Upgrading to a new version of the VPN 3000 Concentrator software does not automatically overwrite the existing configuration file. Configuration options for new features (for example, IKE proposals) are not automatically saved to the configuration file on an upgrade. The HTML Manager displays "Save Needed" (rather than "Save") to indicate that the configuration needs to be saved. If the configuration is not saved, then on the next reboot, the new configuration options are added again. If you need to send the configuration file to the TAC, save the running configuration to the configuration file first.

CFMI - CORR
Fls N° 077
3698

3. Enter a name for the backup file (in 8.3 format; for example, name it CON367BK.TST)

You have now backed up the existing configuration to the flash.

Backing Up the Existing Configuration to an External Server

You should also back up the configuration to a server. You can do this in many ways, one of which is to download the file using your Web Browser from the HTML interface (VPN Manager).

You can now upgrade the software with assurance that you can return to your previous firmware using your previous configuration.

Note After upgrading, be sure to clear the cache on your browser. Release 4.0 adds features and enhances HTML page layouts. Clearing your browser cache ensures that everything displays correctly and uses the new features and layout.

Downgrading from Release 4.0

If you need to return to a release prior to Release 4.0, do the following:

Step 1 Reload the firmware for the desired release. (Do not reboot yet.)

Step 2 Rename the existing configuration (for example, rename it as CON367BK.TST).

Step 3 Delete "CONFIG".

Step 4 Copy the previously saved backup file (for example, CON36BKP.TST) to CONFIG. Do not click Save (otherwise, your original CONFIG file will be overwritten with the running configuration).

Step 5 Perform a software reset.

Your prior firmware and image are restored.

To determine the amount of memory currently installed in your VPN Concentrator, use the Monitoring | Status screen. For information about installing memory upgrades and about updating the VPN Concentrator Manager and the VPN Concentrator Bootcode, see *Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator*, included with your memory upgrade kit.

RADIUS User Filters

With Release 4.0, administrators can define remote access user filters in Cisco Secure ACS as download PIX ACLs or as a Cisco vendor-specific RADIUS attribute AV-PAIR (26/9/1), rather than having to define them on each VPN Concentrator. This feature provides limited support for to download inbound access control lists or filters and apply them to a user or group, rather than defining the filters on the VPN Concentrator.

A network administrator can configure the filters on a RADIUS server, rather than on the VPN Concentrator. To provide information about the filter and filter rules, the VPN Concentrator's management system includes a new screen in the monitoring and administration sessions.

Backup LAN-to-LAN

The Backup LAN-to-LAN feature lets you establish redundancy for your LAN-to-LAN connection. Unlike VRRP, which provides a failover for the VPN Concentrator, Backup LAN-to-LAN provides a failover for the connection itself. Although VRRP and Backup LAN-to-LAN are both ways of establishing continuity of service should a VPN Concentrator fail, Backup LAN-to-LAN provides certain advantages that VRRP does not.

- You *can* configure Backup LAN-to-LAN and load balancing on the same device, but you cannot configure VRRP and load balancing on the same VPN Concentrator.
- Redundant Backup LAN-to-LAN peers do not have to be located at the same site. VRRP backup peers cannot be geographically dispersed,

Note This feature does not work in conjunction with VRRP. If you set up a Backup LAN-to-LAN configuration, disable VRRP.

8572
A.

SNMP Enhancements

With Release 4.0, you can configure a list of particular event identifiers to track, as well as tracking events by class and severity. For more information, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, Chapter 10, "Events."

Disable LAN-to-LAN Tunnels

With Release 4.0, an administrator can disable a LAN-to-LAN VPN connection without deleting its configuration. This feature can be useful for troubleshooting a connection.

Configurable giaddr for Group-Based DHCP

This feature lets an administrator define a network address on a group basis to be used in DHCP proxy address assignments. To use this feature, DHCP proxy must be enabled on the VPN 3000 Series Concentrator. The administrator enters a network address without a subnet mask under group and user configuration. This address indicates to the DHCP server the scope (that is, the range of available IP addresses on the DHCP server) within which to assign the address.

Memory Conservation Enhancements

Release 4.0 includes modifications to memory structures and allocation algorithms to limit unnecessary memory use.

Memory Statistics Display Enhancements

The VPN 3000 Concentrator and the VPN 3002 Hardware Client now monitor and display memory usage in terms of block size and free and used blocks. The display also includes a new page with detailed statistics.

CPMI - CORREIO
Fls Nº 080
Doc 3698

8570
A-

Disable Group Lock When Using SDI or NT Domain Authentication

This feature is supported only when using Internal or RADIUS authentication. To ensure that you are using this feature properly please refer to the following URL: http://www.cisco.com/warp/customer/471/altigagroup.html

Password Expiry Does Not Change User Profile for LAN

You must enable Start Before Logon on the VPN Client and possibly may need to make sure that DNS and WINS servers are properly configured (CSCdv73252).

Browser Interoperability Issues

The following sections describe known behaviors and issues with the indicated Web browsers.

VPN 3000 Concentrator Fully Supports Only Netscape and Internet Explorer

Currently, the VPN 3000 Concentrator fully supports only Netscape and Internet Explorer. Using other browsers might cause unacceptable behavior; for example, if you attempt to use an unsupported Web Browser to manage the VPN 3000 Concentrator, clicking any of the links might return you to the login screen. (CSCdx87630).

Internet Explorer 4.x Browser Issues

The following are known issues with Internet Explorer 4.X and the VPN Concentrator Manager (the HTML management interface). To avoid these problems, use the latest version of Internet Explorer.

- If you encounter a script error when you try to save your configuration file using Internet Explorer 4.0, reinstall Internet Explorer 4.0, or upgrade to a later version of Internet Explorer. Reinstalling Internet Explorer fixes the problem.

081
3698

8568
A

2. The User should be authenticated (using the authentication method of the tunnel group.
3. The User's Group (as defined by the group delimiter option) should be authenticated.

This all works properly, but in the Administration | Administer Sessions screen, the Tunnel Group displays instead of the User's Group (CSCdy00360).

Long Initialization for SNMP Traps in Releases 3.0, 3.5, and 3.5.1

In Releases 3.0, 3.5, and 3.5.1 of the VPN 3000/3002 products, the SNMP task takes 3-5 minutes to complete initialization after a device reboot. Traps being processed during this interval are queued and sent to the SNMP Management station after SNMP task initialization completes.

However, the cold start trap, normally sent as a result of a device rebooting, is never sent.

In Release 2.5.X, the cold start trap is properly sent to the SNMP Manager after a device reboots (CSCdt01583).

Windows NT Authentication Servers Can't Follow Other Server Types in the a Prioritized Authentication Server List

If an Windows NT server follows a non-NT server in the prioritized authentication server list, and the non-NT server becomes unavailable for some reason, the VPN 3000 Concentrator detects this and falls back to the Windows NT server. If the tunnel being established is PPTP or L2TP, the authentication attempt to the Windows NT server also fails.

Therefore, when configuring PPTP or L2TP connections, do not place Windows NT authentication servers behind other types of servers in the applicable authentication server list (CSCdy07226).

CPMI - CORRESPONDANCE
082
File N°
Doc 3698

If the configured rekey interval is very short, users might find repeated authorization requests inconvenient. In this case, disable reauthentication. To check your VPN Concentrator's configured rekey interval, see the Lifetime Measurement, Data Lifetime, and Time Lifetime fields on the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify screen.

Note At 85% of the rekey interval, the software client prompts the user to reauthenticate. If the user does not respond within approximately 90 seconds, the VPN Concentrator drops the connection.

VPN 3000 Concentrator Ignores RADIUS Packets Longer Than 4096 Bytes

Some RADIUS Servers exceed the Maximum RADIUS packet size of 4096 bytes. The VPN 3000 Series Concentrator ignores RADIUS packets that exceed this length (CSCdz90027).

Downgrading to Release 3.6 with a Release 4.0 Configuration Deletes Information from LAN-to-LAN Groups

A VPN Concentrator with more than 125 users and groups combined fails to terminate tunnels if the SEPs are not active. This is because a VPN Concentrator with no active SEPs is considered to be a model 3015, and model 3015 supports only 125 users and groups combined.

This condition could unexpectedly arise if a VPN Concentrator with a SEP-E, running Release 4.0, is downgraded to Release 3.6. This would result in the problem, because the Release 3.6 does not support the SEP-E module. The SEP-Es are detected as unknown cards if present when running Release 3.6 code.

If you encounter a situation, for whatever reason, where you are trying to load a configuration with more users than are supported by the model, the following event appears on the console after a reboot:

****

3 03/20/2003 14:03:16.260 SEV=3 CONFIG/32 RPT=1

083
3698

3564
A.

- CSCdt08303

  When configuring a LAN-to-LAN connection with IOS or PIX, it is important to match the keepalive configuration (both "ON" or both "OFF"). If the keepalive configuration is OFF for the VPN 3000 Concentrator and ON for the IOS device, the tunnel will be established with data.

  IOS tears down the tunnel because the VPN 3000 Concentrator does not respond to IOS style keepalives if keepalives are configured to be OFF for the VPN 3000 Concentrator.

- CSCdw36613

  In some cases, the Zone Labs Integrity Agent may not properly update on the Windows NT version 4.0 operating system while the VPN Client is connected, policy is changed and re-deployed, and the connection is up. Specifically, if you "Block Internet Servers" under the Firewall Security Rules in the Policy and then Deploy that new policy, a PC running Windows NT version 4.0 receives the updated policy, but it might not put the "Block Internet Servers" setting of that policy into effect.

  Workaround:

  Reboot the operating system.

- CSCdx47596

  Due to a Microsoft bug, Windows XP PCs are not capable of receiving a large number of Classless Static Routes (CSR). The VPN 3000 Concentrator limits the number of CSRs that are inserted into a DHCP INFORM message response when configured to do so.

  The VPN 3000 Concentrator limits the number of routes to 28-42, depending on the class.

- CSCdx89348

  The Concentrator may display the following events during a VPN Client connection. These events were found to be due to the client being behind a Linksys Cable/DSL router that was incorrectly modifying the Client's packets, causing them to fail authentication when received by the VPN Concentrator. The problem is more prominent if LZS compression is used.

  Events:

  131500 06/20/2002 17:08:34.300 SEV=4 IPSEC/4 RPT=4632

  IPSec ESP Tunnel Inb: Packet authentication failed, username: gray, SPI:

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 084
Doc. 3698

8562
A.

- CSCdz87108

  The LDAP Authorization failure reasons depend on how the LDAP server implements these error codes. RFC 1777-LDAP states that the LDAP server might not return an error code, therefore in those situations the VPN 3000 failure reason is "Invalid response received from server".

  For the case in which the LDAP server *does* return a specific error diagnostic (for example, noSuchAttribute) the VPN 3000 failure reason displays the appropriate string.

- CSCea20236

  Before you use the VPN Concentrator to authenticate a user to a Linux or Unix server running a Kerberos server, follow these steps:

  a. Check the keys available for the user you want to authenticate. Run:

     kadmin.local -q "getprinc *username*"

  b. Make sure that "DES cbc mode with RSA-MD5, Version 5" is one of the available keys. If you do not see "DES cbc mode with RSA-MD5, Version 5", edit the kdc.conf file and add or move des-cbc-md5 selections to the beginning of the supported_enctypes = line. For example:

     [realms]

     MYCOMPANY.COM = {

     master_key_type = des-cbc-crc

     supported_enctypes = des-cbc-md5:normal des-cbc-md5:norealm des-cbc-md5:onlyrealm

     Save the file. Then, restart the krb5kdc, kadmin, and krb524 services.

  c. To create the "DES cbc mode with RSA-MD5" keys, change the users password:

     kadmin.local -q "cpw -pw newpassword *username*"

  Now you should be able to authenticate that user to your Linux/Unix Kerberos 5 server.

- CSCea29828

  HTTP Software Updates sometimes fail with "Software Update Error". Retrying the operation does not update the image.

  Workarounds:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 085
3698
Doc.

8501
A.

Caveat Resolved in Release 4.0

Release 4.0 resolves the following issues:

- CSCdy09630

  The description of the IPSec Backup Servers feature in the VPN 3000 Concentrator Series Reference documentation indicates that it applies only to the VPN3002 Hardware Client. The feature now applies to the Software Client as well. For information about this feature and how to configure it, on the VPN Concentrator, see *VPN Client Administrator Guide*, Chapter 1. For information about how to configure Backup Servers in the VPN Client, see *VPN Client User Guide*.

- CSCdy12056

  If a LAN-to-LAN tunnel between a VPN 3000 Concentrator and an IOS device is misconfigured and repeatedly fails to establish, then the VPN 3000 Concentrator could enter a state where a reboot is required.

  One way to encounter this problem is to try to setup IOS to handle both LAN-to-LAN tunnels and Remote Access tunnels on the same interface, without breaking the IOS interface into V-LANs. This is a misconfiguration and is not supported by IOS, but it can lead to problems with the VPN 3000 Concentrator.

  This configuration is not supported because IOS does not allow the same crypto map to be used to terminate both LAN-to-LAN tunnels and Remote Access tunnels. In addition, IOS only allows one crypto map to be applied per interface.

  Consequently, if both types of tunnels must be terminated on a single physical interface, that interface must be broken out into V-LANs. Dividing the physical interface in this way enables a different crypto map to be applied to each virtual interface. This in turn enables both types of tunnels to be terminated on the same physical interface while maintaining a valid configuration.

- CSCdy26296

  When viewing bandwidth management statistics via the CLI, with Bandwidth Management enabled and multiple users connected, all user sessions scroll through on the screen without the user being prompted to press space to continue or Q to quit.

RQS nº 03/2005 - CPMI - CORREIOS
0086
Fls. Nº
Doc. 3698

8559
A.

- CSCdz62206

  If you use Active Directory/Kerberos authentication on the VPN 3000 Concentrator and would like to authenticate to a Windows 2000 or .NET Active Directory server, you *must* change *all* the users' Account options to "Use DES encryption types for this account". This is *required* because the Release 4.0 VPN 3000 Concentrator uses DES encryption, but Windows Active Directory uses RC4.

- CSCdz71450

  When using Active Directory/Kerberos for authentication, if the user types in the username or password incorrectly, the VPN 3000 Concentrator simply ends the connection after the first failure. The user should be prompted three times before failing as it does when using Internal, Radius, or NT Domain authentication methods.

- CSCdz77794

  On the Monitoring | Statistics | Authentication and Monitoring | Statistics | Accounting screens, if you click Reset, then all group-based statistics show up with the Group column=Base Group. In order to show group-based statistics again, click Restore.

- CSCdz78109

  SEP-E to SEP-E failover and SEP-E to software failover are *not* supported in Beta releases.

  New connections are not accepted after SEP-E failover with several calls previously connected and passing data.

- CSCdz79541

  Duplicate of CSCdz85139.

- CSCdz83301

  If a simple password is configured under the OSPF tab, in any of the interface configuration pages, the deleted entry will re-appear even after deleting the password, selecting none for OSPF authentication and clicking apply.

- CSCdz84481

  When a user fails authentication due to a restriction placed on the account at the Active Directory server, the VPN 3000 Concentrator Events do not display the reason for the failure. Some restrictions on the account could be

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 087
Doc: 3698

8557
A-

CAPI-RSA PKCS1 payload to be decrypted is not in PKCS1 format, bad block type=[0x7][0xb8].

If you receive this event, you will be unable to use HTTPS to manage the VPN Concentrator. To workaround this problem, delete the SSL certificate (from the Administration | Certificate Management screen), then generate a new SSL certificate.

- CSCea13002

  The functionality that allows the administrator to create a network list, from within a LAN-to-LAN configuration page, has changed.

  In previous releases, the user could create a network list from within the LAN-to-LAN configuration page. The new method for creating a network list uses a link on the LAN-to-LAN index page to the network list configuration page.

  This change was resolves a problem with Reverse Route Injection when the network lists are added from within the LAN-to-LAN page. With the previous method, the routes, corresponding to the network lists that were added via the LAN-to-LAN page, were not present in the routing table.

- CSCea16255

  When Strip Realm is disabled, accounting requests should be sent as user name=user. But instead, accounting requests are incorrectly sent with user name=user@realm (Duplicate of CSCea44988).

- CSCea20412

  Using Authentication=RADIUS with Expiry, the VPN Concentrator establishes the tunnel but skips either RADIUS or LDAP authorization.

- CSCea24328

  When using Kerberos/Active Directory authentication, if a user types a username with the "@" symbol and Realm using all lowercase for the realm (that is, usernam@mycompany.com instead of username@MYCOMPANY.COM), the following error occurs on the VPN Concentrator, and the Kerberos server status changes to "Not-in-service".

  78 02/19/2003 16:59:49.250 SEV=7 AUTHDBG/76 RPT=8
  Unable to correlate received message with authentication session

  83 02/19/2003 16:59:53.150 SEV=4 AUTH/15 RPT=76
  Server name = 100.136.50.2, type = KERBEROS,
  group = KerberosGroup, status = Not-in-service

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 088
3698
Doc:

Inbound Firewall Rules Must Not Limit Traffic to UDP Source Port 4500

In *VPN 3000 Series Concentrator Reference Volume I: Configuration,* Chapter 7, "Tunneling Protocols," make the following change to the note on page 7-35, under Tunneling Protocols | Configuration | System | Tunneling Protocol | IPsec | NAT Transparency area, regarding IPsec over NAT-T:

Note The source port of the client may vary from UDP 4500 especially when traversing a PAT device, so any inbound firewall rules must not specifically limit traffic to a source port of 4500.

VPN 3000 Concentrator Documentation Updates

In addition to these Release Notes, the following documents are new or have been updated for Release 4.0:

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management*
- *VPN 3000 Series Concentrator Getting Started*
- Online Help

Related Documentation

- *VPN Client User Guide for Windows*
- *VPN Client Administrator Guide*
- *VPN 3002 Hardware Client Getting Started*
- *VPN 3002 Hardware Client Reference*
- *VPN 3002 Hardware Client Quick Start Card*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 089
Doc. 3698

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

RQS nº 03/200 25
CPMI - CORREIOS
090
Fls: Nº
3698
Doc.

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

ROS nº 03/2003 - CPMI - CORREIOS
Fls. Nº 091
Doc. 3698

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 092
Doc. 3698

8548
A-

trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 093
Doc. 3698

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 094
Doc. 3698

8552
A.

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0955
Doc.

8554
A

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in "Service and Support" in *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco TAC Home Page

The Cisco TAC home page includes technical tips and configuration information for the VPN 3000 Concentrator and client. Find this information at:

http://www.cisco.com/warp/public/707/#vpn3000.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

RQS nº 03/2005 - CN
CPMI - CORREIOS
096
Fls. Nº
3698
Doc.

- When using Kerberos/Active directory for authenticating, users should enter only their username, username@REALM.COM with Realm all in UPPERCASE letters, or use the Strip Realm setting for the Group on the Concentrator.
- CSCea25668

  Statically assigned filters take precedence over dynamically assigned filters. It should be the other way around.

Documentation Updates

The Cisco VPN 3000 Series Concentrator documentation set has been revised for this release and is available online through Cisco Connection Online (CCO). This section contains any changes and corrections to the documentation that occurred after the documentation was published.

Documentation Changes

The following document requires modifications, reflecting product changes, as noted in the following sections:

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*

Changes to *VPN 3000 Series Concentrator Reference Volume I: Configuration*

Please note the following changes to the Configuration manual.

Syslog Servers Now Supported on Both Windows and UNIX Operating Systems

The VPN 3000 Concentrator now supports syslog servers on both Windows and UNIX (Linux and Solaris) operating system platforms. In *VPN 3000 Series Concentrator Reference Volume I: Configuration,* Chapter 10, "Events," and in the corresponding online Help, the text and the screen captures refer to UNIX syslog servers. This restriction on the type of syslog server operating environment no longer exists.

78-15416-01
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 097
Doc. 3698

3558
A.

Account Expired, Account Disabled, Account Locked-Out, Not within Logon Hours and Password Change required. For most of these restrictions you will see the following Events:

124 01/20/2003 11:12:55.590 SEV=10 AUTHDECODE/43 RPT=4

Kerberos: Error type: Client's creds have been revoked

130 01/20/2003 11:12:55.590 SEV=4 AUTH/9 RPT=9 70.139.1.5

Authentication failed: Reason = Invalid response received from server handle = 196, server = 198.133.219.25, user = myuser

- CSCdz85139

  When you add an LDAP Authorization server, the events refer to the server with "type=TACACS+."

- CSCdz87048

  The VPN 3000 Concentrator may leak memory when a VPN Client connects and downloads and ACL User Filter from the RADIUS Server. The amount of memory leaked is closely associated with the size of the actual filter.

- CSCdz87381

  If you externally authenticate Groups and Users to a RADIUS Server, the User filters assigned by the RADIUS Server get corrupted. It is recommended that you authenticate the Groups locally on the Concentrator and the Users externally on a RADIUS Server when utilizing the RADIUS User Filter feature.

- CSCea02122

  RADIUS based user filters are not cleared from the Concentrator when PPTP or L2TP connections are terminated.

- CSCea03407

  Using Netscape version 4.7, under Admin | Admin Sessions, the RADIUS User ACL filters get displayed in a narrow 1 inch wide column with no scroll capabilities. The filters are displayed correctly under Monitoring | Dynamic filters.

- CSCea12148

  If your VPN Concentrator has a SEP-E installed, you might see the following event message when you boot:

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 098
Doc. 3698

3560

A•

- CSCdy28464

  Documentation for the Bandwidth Management feature in Release 3.6.1 refers to a configuration option in which bandwidth aggregation is automatically applied to a LAN-to-LAN connection when a bandwidth reservation policy is applied to a LAN-to-LAN connection. This feature is not available in Release 3.6.1.

  To ensure that bandwidth is always available for a LAN-to-LAN connection via the HTML interface, navigate to Configuration | User Management | Groups. Highlight the LAN-to-LAN group, and select the Assign Bandwidth Policies button. Select the public interface, and next to the Bandwidth Aggregation parameter, enter the amount of bandwidth to reserve from the total available bandwidth for this connection.

  If bandwidth aggregation is not set for a LAN-to-LAN connection, a situation might occur where there is not enough bandwidth available for the tunnel to be established.

- CSCdz48220

  The VPN 3000 Concentrator continually requests the node secret from the RSA server. The RSA server considers these requests as failed login attempts by the RSA server; therefore, the user's account is disabled.

  This problem occurs under the following conditions:

  - The VPN 3000 Concentrator does not have the node secret stored locally.
  - The VPN Client provides an incorrect passcode.

- CSCdz48332

  If you add and delete filters through the GUI interface (Configuration |System |Policy Management | Traffic Management | Filters), there is a very small memory leak for each filter created and deleted.

- CSCdz48402

  The VPN 3000 Concentrator does not consistently send Delete with Reason messages to all the connected clients when you do Reboot *NOW*. The VPN Clients believe they are still connected, but they will eventually disconnect due to the Client's Dead-Peer-Detection mechanism.

- CSCdz53656

  Authorization server statistics are not available in this release.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 099
3698
Doc.

8562
A

Do *one* of the following:

- Perform the Software Update using the CLI/telnet interface.
- Reboot the VPN 3000. Performing an HTTP Software Update will now succeed.

- CSCea46018

  When a backup SEP-E fails over to Software, the Activity LED and Status LED stay green, even though the SEP-E is no longer operational.

- CSCea52820

  The text from the Help page for the Monitoring | System Status | Memory Details page in HTML incorrectly refers to "Memory Detail Report". The page is labelled and called: "Detailed Memory Report".

- CSCea52936

  The Help for the SEP-E in the Monitoring | System Status | SEP in-line SEP page is incomplete. In other sections, we make reference to the SEP-E. We should add:

  "AES (SEP-E only)" to the Encryption and Decryption bullet.

  This screen displays status and statistics for a VPN Concentrator SEP (Scalable Encryption Processing) or a SEP-E (Enhanced SEP) module, which performs hardware-based cryptographic functions:

  - Random-number generation.
  - Hash transforms (MD5 and SHA-1) for authentication.
  - Encryption and decryption (DES and Triple-DES).

  The screen shows cumulative data since the system was last booted or reset.

- CSCea69156

  LDAP Authorization to a Microsoft Active Directory LDAP server using authenticated Bind requests is not supported in this release. Only anonymous Binds are currently supported.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 100
Doc: 3698

8563
A

4e01db67, Seq Num: 0000850f. Dump of failed hash follows.

Linksys has been notified about the problem.

Workaround:

Although no workaround currently exists, disabling LZS compression on the Concentrator helps reduce the number of events. To disable LZS compression on the Concentrator set the "IPComp" setting on the IPSec tab of the group configuration to "none".

- CSCdy26161

  The Microsoft L2TP/IPSec client for Windows 98, Windows ME, and Windows NT does not connect to the VPN 3000 Concentrator using digital certificates.

  Workaround:

  Use Preshared keys.

- CSCdy27564

  The Assigned IP address for a PIX-501 in Network Extension Mode appears on the VPN 3000 Concentrator as 0.0.0.0 until the first IPSec/Phase 2 rekey takes place. After the Phase 2 rekey completes, the Assigned IP address is correctly set to the PIX-501's private interface network address.

- CSCdz24882

  Using Microsoft Internet Explorer version 5.0, you cannot create a detailed memory report from the Monitoring | System Status | Memory Status | Detailed Memory Report button. The file memory.txt is *not* created. The report does work if the file already exists. You *can* create the file initially if you run a detailed report from the CLI interface. Internet Explorer version 5.5 and Netscape work fine.

- CSCdz83332

  When switching between tabs under the interfaces section of the html-management page, the action may eventually fail.

  If this happens simply go back to the interface summary page and drill back down into the desired interface. Everything will resume working again.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 101
Doc: 3698

8565
A-

SERVE Too Many Entries Error. Delete an entry before adding a new one.

****

(CSCea51435)

VPN Client Supports Elevated Privileges Using the MSI Installer

Windows Installer 2.0 must be installed on a Windows NT or Windows 2000 PC prior to configuring the PC for a Restricted User with Elevated Privileges When using elevated privileges, the VPN Client program files are created under the specific user, not "ALL" users. (CSCea37900).

Open Caveats for VPN 3000 Series Concentrator

Caveats describe unexpected behavior or defects in Cisco software releases. The following list is sorted by identifier number.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

The following problems exist with the VPN 3000 Series Concentrator, Release 4.0.

- CSCds44095

  L2TP over IPSec connections fail if going through a NAT device. During the connection establishment, the VPN Client and the VPN 3000 Concentrator exchange IP addresses. When the client sends what it believes to be the VPN 3000 Concentrator's address (really the NATed address), the VPN 3000 Concentrator releases the connection.

  This is because the address assigned to the interface does not match the address coming in from the client. The same issue exists on the client side. This will not be resolved until the Windows 2000 MS client supports UDP encapsulation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 102
3698
Doc.

3567
A

Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

"The page cannot be displayed."

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

SNMP Traps VRRP Notifications and cipSecMIBNotifications Are Not Supported

The VPN 3000 Concentrator does not support the VRRPNotifications and cipSecMIBNotifications SNMP traps. You can configure VRRP for these SNMP traps without getting an error message, but the traps themselves are not supported, so no action occurs. The same is true of Cisco IPSec-flow MIB notifications (CSCdx44580).

RSA Allows a CA to Issue Only One Certificate with any DN

The rekey option to renew an SSL certificate from the RSA CA results in a rejection of the request.

The resubmit/renew feature does work with RSA as long as the certificate being rekeyed or renewed is first deleted from the CA database. RSA does not allow a CA to issue more than 1 certificate with any particular DN (CSCdv27743).

Reauthentication on Rekey Interval

If you have enabled the Reauthentication on Rekey feature, the VPN Concentrator prompts users to enter an ID and password during Phase 1 IKE negotiations and also prompts for user authentication whenever a rekey occurs. Reauthentication provides additional security.

78-15416-01
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 103
Doc. 3698

- If you plan to upgrade the firmware on multiple VPN Concentrators at the same time from the same PC, use the version of Internet Explorer on the Cisco VPN 3000 software distribution media or newer. Using an earlier version could cause a failure in one or more of the upgrades.
- When connecting to the VPN Concentrator using SSL with Internet Explorer 4.0 (v4.72.2106.8), you might receive a message box saying, "This page contains both secure and non-secure items. Do you want to download the non-secure items?" Select Yes. There really are no *non-secure* items on the page and the problem is with Internet Explorer 4.0. If you upgrade to Internet Explorer 4.0 Service Pack 1 or Service Pack 2, you should not see this error message again.

  After adding a new SSL certificate, you might have to restart the browser to use the new certificate.

VPN Client Used with Zone Labs Integrity Agent Uses Port 5054

VPN Clients, when used with the Zone Labs Integrity Agent, are put into a "restricted state" upon connection to the Integrity Server if a port other than 5054 is used. The restricted state simply means the VPN Client is able to communicate only with the Integrity Server; all other traffic is blocked (CSCdw50994).

Workaround:

Do *one* of the following:

- Configure the VPN Concentrator and the Integrity Server to use port 5054 when communicating with each other.
- Edit the WEB.XML file in the Integrity directory and search for 5054 (the port that Integrity uses/looks for). Change it to 5000, save, and restart the Integrity Server.

Administer Sessions Screen Shows Data for Wrong Group

When an L2TP/IPSec connection is established, authentication should behave as follows:

1. The Tunnel Group is authenticated (using the OU field in the Certificate or using the Base Group).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 104
Doc. 3698

Enhanced Sygate Firewall AYT Support

Release 4.0 includes support for Sygate Personal Firewall, Sygate Personal Firewall Pro, and Sygate Security Agent.

Enhanced PING Command Features

Admin users who have only read access can now do PING commands, using either the Monitor tab on the GUI or the command-line interface. The PING command also appears, as before, on the Admin tab, accessible to users who have full access privileges. The PING command now shows the reply time in milliseconds and not just "device is available."

Adjustable DPD Timeout

For dead-peer detection (DPD), this feature lets an administrator configure the interval that the Concentrator waits before beginning Keepalive monitoring. This feature applies only to Easy VPN Clients that are using IKE Keepalives.

Usage Notes

This section lists interoperability considerations and other issues to consider before installing and using Release 4.0 of the VPN 3000 Series Concentrator software.

Online Documentation

The online documentation might not be accessible when using Internet Explorer with Adobe Acrobat, Version 3.0.1. To resolve this issue, upgrade to Acrobat 4.0 or higher. The latest version of Adobe Acrobat is available at the Adobe web site: http://www.adobe.com.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 105
Doc. 3698

8573
A-

Native Kerberos Authentication

Release 4.0 supports authentication to Kerberos/Active directory, which is the default authentication mechanism in Windows 2000 and Windows XP. Kerberos is an authentication protocol for use on untrusted networks. The protocol comprises two stages of authentication--the first level is to a key distribution center (KDC), and the second level is between each client and server.

To configure this feature, an administrator must add a Kerberos authentication server on a group basis or add the server to the global authentication servers list and configure such parameters as server IP address, server port, number of retries, and so on. The IPSec group tab includes Kerberos as an authentication type, and statistical displays also include Kerberos authentication statistics.

See the Open Caveats section for information about configuration issues with Active Directory (CSCdz62206) and Linux/UNIX (CSCea20236).

LDAP/RADIUS Authorization

This feature separates user authorization (permissions) from user authentication. It lets certificate users receive permissions by means of LDAP or RADIUS without secondary authentication via XAUTH. It also lets non-certificate users using any type of authentication scheme (Kerberos, NT Domain, SDI, Radius, and Internal) to retrieve these permissions/attributes.

The feature provides a way to configure RADIUS and LDAP authorization servers and event information. The network administrator configures authorization servers on a global system or group basis.

Alerts (Delete with Reason Notifications)

The VPN 3000 Concentrator and the VPN 3002 Hardware Client can send alerts with reasons for disconnects and reboots they initiate to either the VPN Client or Concentrator to which they connect. When a disconnect occurs, the VPN Client displays the disconnect notice and the reason (if available) in the Event log.

The VPN Client can also send alerts regarding disconnects that it initiates, but it does not send a reason.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 106
Doc: 3698

8515
A-

New Features in Release 4.0

This section describes the new features in Release 4.0 of the VPN 3000 Series Concentrator. For detailed instructions about how to configure and use these features, see *VPN 3000 Series Concentrator Reference Volume I: Configuration* and *VPN 3000 Series Concentrator Reference Volume II: Administration and Management.*

Hardware Acceleration for Advanced Encryption Standard (AES)

VPN 3000 Concentrator models 3015 and higher now offer an enhanced, scalable encryption processor (SEP-E), that provides hardware support for AES (software support was added in Release 3.6). This feature has no configuration implications. For installation information about the new SEP-E modules, see *Installing SEP or SEP-E Modules in the VPN 3000 Series Concentrator.*

Note The VPN 3000 Concentrator uses *either* SEP or SEP-E modules, not both. Do not install both on the same device. If you install a SEP-E module on a VPN Concentrator that already contains a SEP module, the VPN Concentrator disables the SEP module and uses only the SEP-E module.

512 MB On-Board Memory

You can now upgrade your VPN 3060 or 3080 Concentrator memory to 512 MB.

Note To take advantage of this additional memory, you must also update the VPN Concentrator Manager to Version 4.0 and update the VPN Concentrator Bootcode to Version 4.0.

If your VPN 3000 Concentrator is running low on memory resources, upgrading to 512 MB will help. Symptoms that indicate low memory include the following:

- VPN Concentrator cannot support the necessary number of tunnels.
- VPN Concentrator cannot accept additional connections.
- VPN Concentrator crashes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 107
3698
Doc.

Before You Begin

Before you upgrade to this release, *back up your existing configuration to the flash and to an external server.* This ensures that you can return to the previous configuration and software if you need to.

Be aware of the following considerations before you upgrade. These are known product behaviors, and your knowing about them at the beginning of the process should expedite your product upgrade experience. Where appropriate, the number of the caveat documenting the issue appears at the end of the item. See Open Caveats for VPN 3000 Series Concentrator, page 16 for a description of using this number to locate a particular caveat.

Release 4.0 of the VPN 3000 Concentrator software contains several features that interact with corresponding new features in the Release 3.6.x versions of the VPN Client and VPN 3002 Hardware Client software. To get the full benefit of this release you should upgrade your client software as well as your concentrator software. The VPN 3000 Concentrator software, Release 4.0, does operate with VPN Client and VPN 3002 Hardware Client versions 3.0 and higher, but you should upgrade these, too, to take full advantage of the new features.

- To use the VPN Client, Release 3.0 or higher, you *must* upgrade the VPN Concentrator to Release 3.0 or higher. The VPN Client, Release 3.0 or higher, does *not* operate with the VPN 3000 Concentrator version 2.5 or earlier versions.
- Do not update the VPN 3000 Concentrator when the system is under heavy use, as the update might fail (CSCdr61206).
- If you are upgrading from Release 3.0 to Release 3.1 or higher and you are using the "Group Lookup" feature, you must manually set Group Lookup after the upgrade. To enable this feature, go to Configuration | System | General | Authentication and select the Enable check box (CSCdu63961).

Use the following backup procedure to ensure that you have a ready backup configuration.

Backing Up the Existing Configuration to the Flash

1. Go to Administration | File Management | Files.
2. Select the configuration file and click Copy.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 108
3698
Doc.

8579
A

section, "Usage Notes," describes interoperability considerations and other issues you should be aware of when installing and using the VPN 3000 Series Concentrator. Read these release notes carefully prior to installing this release.

Contents

These release notes describe the following topics:

System Requirements, page 2

Upgrading to Release 4.0, page 3

New Features in Release 4.0, page 6

Usage Notes, page 10

Open Caveats for VPN 3000 Series Concentrator, page 16

Caveat Resolved in Release 4.0, page 21

Documentation Updates, page 26

Obtaining Documentation, page 28

Obtaining Technical Assistance, page 30

System Requirements

This section describes the system requirements for Release 4.0.

Hardware Supported

Cisco VPN 3000 Series Concentrator software Release 4.0 supports the following hardware platforms:

- Cisco VPN 3000 Series Concentrators, Models 3005 through 3080
- Altiga Networks VPN Concentrators, Models C10 through C60

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 109
Doc. 3698

Apensado ao

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 110
Doc. 3698

8547
A.

CHAPTER 5

Customizing the VPN Client Software

This chapter explains how to replace the Cisco Systems brand with your own organization's brand. When you install and launch the VPN Client software, you see your own organization name, program name, and application names on menus, windows, dialogs, and icons.

For the Windows platform, it also explains how to set up the software so that your users can install it automatically without being prompted. This feature is called *silent install*.

To customize the VPN Client software, you create your own distribution image combining the following elements, which this chapter describes.

For all platforms, you can customize the following:

- Cisco Systems image that you receive on the Cisco Systems software distribution CD.
- Your own portable network graphics (PNG) (Table 5-2) and icon files to replace the Cisco Systems brand.
- A vpnclient.ini file for configuring the VPN Client software globally (see Chapter 2, "Preconfiguring the VPN Client for Remote Users").
- Individual profile (.pcf) files for each connection entry (see Chapter 2, "Preconfiguring the VPN Client for Remote Users").

For the Windows platform, you can also customize the following:

- An oem.ini file that you create. Cisco supplies a sample oem.ini file that you can use as a template and customize.
- setup.bmp—a bitmap file that displays on the first InstallShield® window when you install the VPN Client. (InstallShield only)

These elements should all be in the same directory and folder. Because some of the files may be too large to distribute the oem software on diskettes, we recommend that you make a CD ROM distribution image.

CPMI - CORREIOS
Fls. Nº 111
Doc. 3698

8546
A.

Customizing the VPN Client GUI for Windows

This section describes how to customize the VPN Client GUI for the Windows platform. To customize the GUI for the Mac OS X platform, see Customizing the VPN Client GUI for Mac OS X, page 5-18.

Customizing the VPN Client occurs when the VPN Client and installation program see a text file called oem.ini on your distribution image. The oem.ini file is patterned after Microsoft standard initialization files. You create the oem.ini file and supply your own text, PNG files, and icon files. When present, the oem.ini, PNG, and icon files are read when you first start the VPN Client. Since the VPN Client software reads these files when it first starts, the changes to them take effect only *after* you restart the VPN Client application.

This chapter contains the following sections:

- Areas Affected by Customizing the VPN Client
- Creating the oem.ini File
- Installing the VPN Client Without User Interaction
- Customizing the VPN Client Using an MSI Transform

Areas Affected by Customizing the VPN Client

Customizing replaces the following screen text, bitmaps, and icons.

- Brand names on dialog boxes
- Product names on dialog boxes
- Organization logo on all dialog boxes
- Graphic at the left end of the title bar
- Icons on the system tray (at the bottom right of the screen) and the desktop (shortcut)

Installation Bitmap

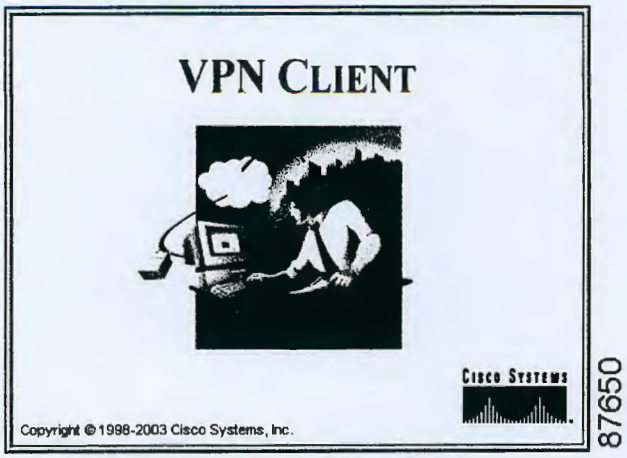
The InstallShield uses a bitmap when installing the VPN Client software: the setup bitmap (setup.bmp).

Figure 5-1 shows the setup bitmap that displays as the first screen during installation via InstallShield.

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-15404-02
Fls. Nº 112
Doc. 3698

8545
A.

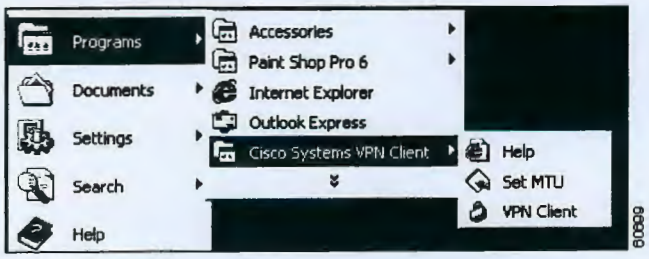
Figure 5-1 Setup Bitmap



Program Menu Titles and Text

After installation, your organization or company, product, and application names appear in the Cisco Systems VPN Client applications menu. (See Figure 5-2.)

Figure 5-2 Applications menu



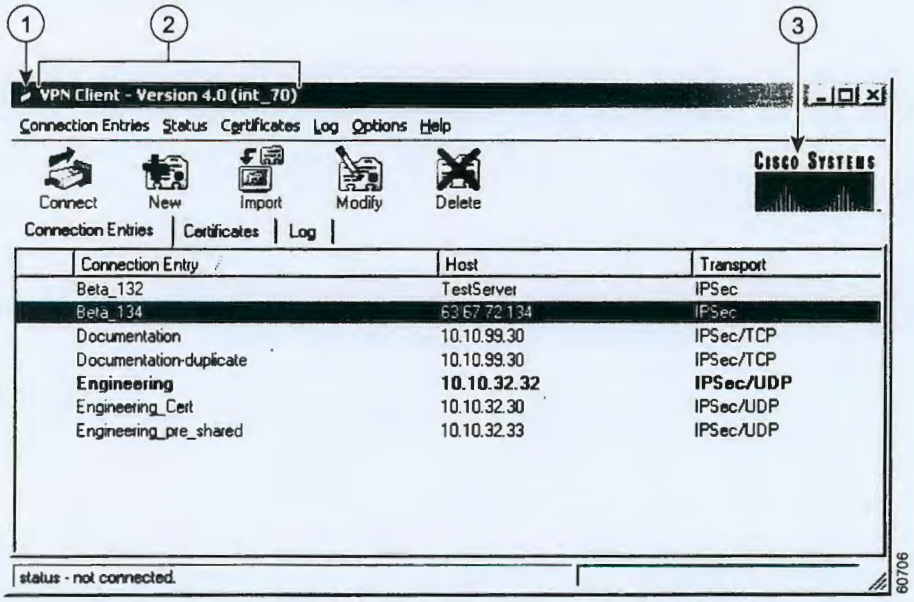
Fls. Nº 113
3698
Doc.

8544
A-

VPN Client

Figure 5-3 shows a lock image (title_bar.png), window title (AppNameText in the oem.ini file), and organization logo (logo.png file). The oem.ini file can replace the window title, the image at the left end of the title bar, and the organization or company logo in the VPN Client software. It can replace the open lock and closed lock icons in the system tray (see Figure 5-4 and Figure 5-5).

Figure 5-3 Three Types of Branding Changes



1	Title bar lock image (title_bar.png)	3	Organization logo (logo.png)
2	Window title (oem.ini file)		

Figure 5-4 Closed Lock Icon on System Tray (connected.ico)

Figure 5-5 Open Lock Icon on the System Tray (unconnected.ico)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 114
3698
Doc.

8543
4.

Setup Bitmap—setup.bmp

The InstallShield version of VPN Client includes a bitmap on the distribution CD that is not in the oem.ini file: `setup.bmp`. You can substitute your own image for this .bmp file, as long as you keep the current filename (setup.bmp) and make sure that the file is in the same directory and folder as the oem.ini file. This file displays a logo on the window when you start the InstallShield installation program. The size of the Cisco Systems setup bitmap is 330x330 pixels and it uses 256 colors.

Creating the oem.ini File

Your distribution CD must contain the oem.ini file for customizing. The oem.ini file contains the locations and names of bitmaps, icons, window titles, and screen text needed for customizing, all of which need to be in the same directory. When you install or start the VPN Client, the software checks to see if there is an oem.ini file. If so, the software scans it for bitmaps, icons, and text. If the oem.ini file lacks an element (for example, text for the product name), then the software uses whatever you have specified in the default section of the file. If no oem.ini file exists, the software defaults to Cisco Systems bitmaps, icons, and text.

Use Notepad or another ASCII text editor to create the oem.ini file and enter brand text and the names of your bitmap and icon files. See Table 5-1.

Note You can edit the oem.ini file that Cisco Systems supplies.

The format of the oem.ini file is the same as a standard Windows `ini` file:

- Use a semicolon (;) to begin a comment.
- Set values by entering `keyword=value`.
- If you don't specify a value for a keyword, the application uses the default.
- Keywords are not case-sensitive, but using upper and lowercase makes them more readable.

Sample oem.ini File

```
; This is a sample oem.ini file that you can use to overwrite Cisco Systems
; brand name on windows, bitmaps, and icons with your organization's brand
; name.
;
; This file has five sections: [Main],[Brand], [Default], [Dialer], and [SetMTU]
; Each section has keywords designating parts of the interface that the file replaces.
;
; The [Main] section determines whether kerberos uses TCP or UDP (the default).

[Main]
DisableKerberosOverTCP = 1

; The [Brand] section controls window titles during installation and in the
; destination folder for the product and applications.
;
[Brand]
CompanyText = Wonderland University
ProductText = Wonderland Client

;
; The [Default] section establishes the default bitmap and icon to use if
```


CPMI - CORREIOS
Fls. Nº 115
3698
Doc.

```
; assignments are left blank. This section also sets up silent installation.
; Silent mode installation proceeds without user intervention.
;
[Default]
SilentMode = 1
InstallPath = C:\Program Files\Wonderland University\Wonderland Client
DefGroup = Wonderland Client
Reboot = 1
;
; The [Dialer] section controls the text and icons for the dialer software.
; AppNameText appears on the application selection menu. DialerBitMap
; appears on connection windows. AllowSBLLaunches controls whether a remote user can
; launch an application before connecting and logging on to a Windows NT platform.
;
[Dialer]
MainIcon is_install.ico
AppNameText = Wonderland Dialer
AllowSBLLaunches = 0
;
; The [Set MTU] section controls the text and icon for the
; Set MTU applications. AppNameText appears on the application
; selection menu and the title screen. MainIcon appears on the window title.
; bar.
;
[Set MTU]
AppNameText = MTU Setter Application
MainIcon = MtuIcon.ico
AutoSetMtu = 1
SetMtuValue = 1300
MTUAdjustmentOverride = 144
```

oem.ini File Keywords and Values

Table 5-1 describes each part of the oem.ini file.

Table 5-1 oem.ini File Parameters

Keyword	Description	Value
[Main]	Optional field that identifies a section of the OEM.ini file to address special circumstances.	Keep exactly as shown.
DisableKerberosOverTCP=	InstallShield only When installing the VPN Client on Windows, the installation program sets a registry value that forces windows to use Kerberos over TCP instead of UDP, the default. Some NAT devices, such as Linksys, do not support out-of-order IP fragments, which breaks Kerberos. With TCP, fragmentation is not required.	After the keyword and equal sign, enter either 1 or 0. 0 = keep the default, which is to force Kerberos to use TCP. 1 = prevent Kerberos from using TCP.
[Brand]	Required field that identifies the branding text that appears on window titles and descriptions throughout the client application.	Keep exactly as shown, as the branding section of the file.
CompanyText=	Identifies the name of your organization. If not present, the default is "Cisco Systems."	After the keyword and equal sign, enter the organization's name. The name can contain spaces and is not case sensitive.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 116
3698
Doc.

8543
A.

Table 5-1 oem.ini File Parameters (continued)

Keyword	Description	Value
ProductText=	Identifies the name of the application. If not present, the default is "VPN Client."	After the keyword and equal sign, enter the product name. The name can contain spaces and is not case sensitive.
[Default]	Required field that identifies the section that contains names of default bitmap and icon to use if values are blank.	Enter exactly as shown, as the default section of the file.
SilentMode=	InstallShield only Specifies whether to activate silent installation.	After the keyword and equal sign, enter either 0 or 1. 1 activates silent installation: 0 = prompt the user during installation. 1= do not prompt the user during installation.
InstallPath=	InstallShield only Identifies the directory into which to install the client software.	After the keyword and equal sign, enter the name of the directory in the suggested format: *root:\programs\company\product*
DefGroup=	InstallShield only Identifies the name of the folder to contain the client software.	After the keyword and equal sign, enter the name of the destination folder in the suggested format: *foldername*
Reboot=	InstallShield only Specifies whether to restart the system after the silent installation. If SilentMode is on (1) and Reboot is 1, the system automatically reboots after installation finishes.	After the keyword and equal sign, enter 0, 1, or 2: 0 = display the reboot dialog. 1 (and SilentMode = 1) = automatically reboot the system when installation finishes. 2 (and SilentMode = 1) = do not reboot after installation finishes.
[Dialer]	Required field that identifies the section that contains the name of the Dialer application, the bitmap to use on the connections window, and the connection icons.	Enter exactly as shown, as the Dialer section of the file.
AppNameText=	Identifies the name of the dialer application.	After the keyword and equal sign, enter the name of the dialer application. The name can contain spaces and is not case sensitive.
MainIcon=	This is used only by InstallShield for shortcuts to the vpngui.exe.	After the keyword and equal sign, enter the name of the icon file.
AllowSBLLaunches	InstallShield only Specifies whether a VPN Client user is allowed to launch a third party application before logging on to a Windows NT platform.	After the keyword and equal sign, enter 1 to enable or 0 to disable this feature. The default is 0 (to disable). (See Note after table.)
[Set Mtu]	Required field that identifies the section that contains the name of the Set MTU application, the name of the Set MTU icon, and other settings.	Enter exactly as shown; identifies the Set MTU section of the file.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 117
Doc 3698

Table 5-1 oem.ini File Parameters (continued)

Keyword	Description	Value
AppNameText=	Identifies the name of the Set MTU application.	After the keyword and equal sign, enter the name you want to give to this application. The name can contain spaces and is not case sensitive.
MainIcon=	Identifies the icon for the Set MTU title bar, About window, and applications menu. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the icon (.ico) file for this icon.
AutoSetMtu=	InstallShield only Identifies whether to automatically set the MTU for all adaptors during installation using SetMTUValue.	After the keyword and equal sign, enter a value 0 or 1: 0 = do not set MTU; do not launch. 1 = set MTU and silently launch during installation. This is the default
SetMTUValue=	InstallShield only Identifies the value to be used for all adapters bound to TCP/IP	After the keyword and equal sign, enter a value between 64 and 1500, inclusive. The default = 1300.
MTUAdjustOverride=	InstallShield only; Windows NT-based only. Identifies the DNE MtuAdjustment parameter. This value identifies the amount the NIC's MTU is reduced.	After the keyword and equal sign, set to a value between 0 and 1300, inclusive. To use the SetMTU application to set the MTU for the TCP/IP protocol, set this parameter to 0.

Note When AllowSBLLaunches is 0, "Allow launching of third party applications before logon" under Windows Logon Properties is unavailable. There might be cases when you need to launch an application before starting your connection, for example, to authenticate your access credentials. In this case you can use the following procedure:
In the VPN Dialer program, choose **Options > Windows Logon Properties**.
Uncheck **Disconnect VPN connection when logging off**.
Log out.
Log in with cached credentials.
Make your VPN Dialer connection.
Log out.
Log in again while already connected.

Table 5-2 lists the GUI image (portable network graphic) files that the VPN Client uses. If you want to replace any of them with your own image files, you must name your image files exactly as shown in the list; otherwise, the VPN Client GUI does not recognize them.

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-15404-02
Fls. Nº 118
Doc. 3698

8539
A-

Table 5-2 Portable Network Graphic Files

PNG File	Description
splash_screen.png	Splash screen that appears for 2 to 5 seconds when the GUI starts. This screen contains a logo, product name and version, and copyright information.
title_bar.png	Image at the left end of the title bar
connected.png	Image next to connection entry when connection is active
logo.png	Organization logo for simple and advanced mode main dialogs
password_logo.png	Organization logo for password dialog (XAuth), group name and password)
profile_logo.png	Organization logo for new/modify profile dialog
status_down_arrow.png	Down arrow on the status bar of advanced mode, used to change the status bar display
cancel.png	Cancel button on advanced mode connection entries toolbar
connect_pressed.png	Connect button pressed on advanced mode connection entries toolbar
disconnect.png	Disconnect button on advanced mode connection entries toolbar
disconnect_pressed.png	Disconnect button pressed on advanced mode connection entries toolbar
new_profile.png	New button on advanced mode connection entries toolbar
new_profile_pressed.png	New button pressed on advanced mode connection entries toolbar
import_profile.png	Import button on advanced mode connection entries toolbar
import_profile_pressed.png	Import button pressed on advanced mode connection entries toolbar
modify_profile.png	Modify button on advanced mode connection entries toolbar
modify_profile_pressed.png	Modify button pressed on advanced mode connection entries toolbar
delete_profile.png	Delete button on advanced mode connection entries toolbar
delete_profile_pressed.png	Delete button pressed on advanced mode view certificates toolbar
import_certificate.png	Import button on advanced mode view certificates toolbar
import_certificate_pressed.png	Import button pressed on advanced mode view certificates toolbar
export_certificate.png	Export button on advanced mode view certificates toolbar
export_certificate_pressed.png	Export button pressed on advanced mode view certificates toolbar
delete_certificate.png	Delete button on advanced mode view certificates toolbar
delete_certificate_pressed.png	Delete button pressed on advanced mode view certificates toolbar
enroll_certificate.png	Enroll button on advanced mode view certificates toolbar
enroll_certificate_pressed.png	Enroll button pressed on advanced mode view certificates toolbar
verify_certificate.png	Verify button on advanced mode view certificates toolbar
verify_certificate_pressed.png	Verify button pressed on advanced mode view certificates toolbar
show_certificate.png	Show button on advanced mode view certificates toolbar

DOC 08/03/2005 - CN
CPMI - CO
Fls. Nº 119
Doc. 3698

Table 5-2 Portable Network Graphic Files (continued)

PNG File	Description
show_certificate_pressed.png	Show button pressed on advanced mode view certificates toolbar
enable_log.png	Enable button on advanced mode connection entries toolbar
enable_log_pressed.png	Enable button pressed on advanced mode view log toolbar
disable_log.png	Disable button on advanced mode view log toolbar
disable_log_pressed.png	Disable button pressed on advanced mode view log toolbar
clear_log.png	Clear button on advanced mode view log toolbar
clear_log_pressed.png	Clear button pressed on advanced mode view log toolbar
options_log.png	Options button on advanced mode view log toolbar
options_log_pressed.png	Options button pressed on advanced mode view log toolbar
show_log.png	Show button on advanced mode view log toolbar
show_log_pressed.png	Show button pressed on advanced mode view log toolbar
arrow_up.png	Up Arrow button in Backup Servers tab of the new/modify profile dialog
arrow_down.png	Down Arrow button in Backup Servers tab of the new/modify profile dialog

You can also replace the following icon files (as long as your icon files have these same names):

- connected.ico—the tray icon when connected (also in resource file for vpngui.exe icon)
- unconnected.ico—the tray icon when not connected
- disconnecting.ico—the tray icon when disconnecting

Customizing the VPN Client Using an MSI Transform

This section describes how to customize VPN Client installation using a transform for the MSI. To customize the applications, you need *both* a transform and an oem.ini file.

Caution Do not modify the MSI file. To customize MSI, use a transform. Failure to follow recommended procedure will limit the level of support you can expect from Cisco.

Creating the Transform

To create the transform, you edit the vpnclient_en.msi file. You can create the transform with any commercially available MSI installation package, such as Wise or InstallShield. The procedure in this section uses the Microsoft ORCA editor available from the Microsoft Windows Installer SDK. The version used here is from Microsoft Platform SDK November 2001. So before you begin, make sure that ORCA is installed on your system. If you need information on transforms and ORCA, refer to the ORCA documentation.

Here is the procedure:

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-15404-02
Fls. Nº 120
Doc. 3698

8537
A-

Step 1 Start ORCA.

Step 2 Select **File > Open** and enter **vpnclient_en.msi**.

Step 3 Select **Transform > Apply Transform** and select **oem.mst**, the transform template.

To customize oem.mst, you modify some of the information you see in the tables. The parts to modify have green change bars on the left side of the row. Figure 5-6 shows a partial oem.mst file.

Figure 5-6 Editing the Tables in a Transform File

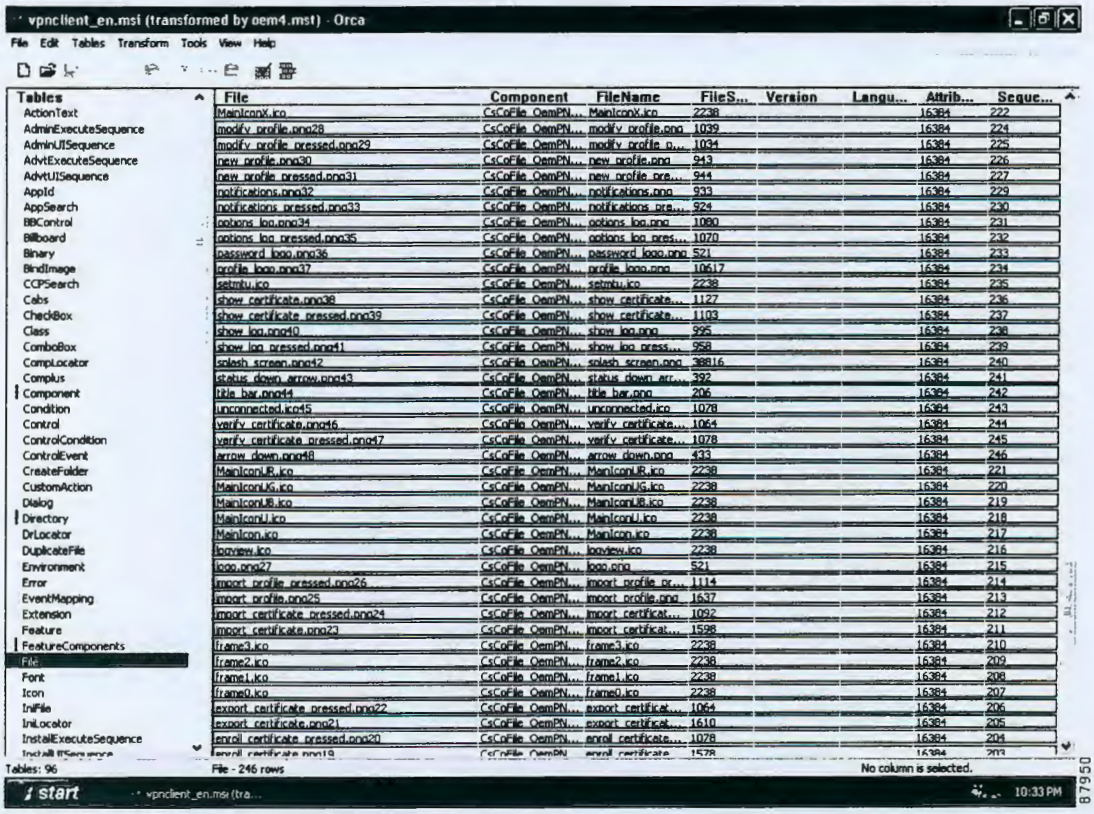


Table 5-3 outlines the changes to make in the tables in the oem.mst file. The columns in the table are defined as follows:

- Table Name—the name of the table to edit
- Changes Needed—a list of the changes to make to the table
- Install Requirement—the entries that modify the installation software
- Client Requirement—the entries that modify the way the VPN Client operates at runtime

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 121
Doc. 3698

Table 5-3 Oem.mst Tables

Table Name	Changes Needed		Modifies Install Parameters	Modifies VPN Client Runtime Parameters
Binary	top16—Add your own 500x63 bitmap for the MSI Install side16—Add you own 501x314 bitmap for the MSI Install		Yes for both	No for both
Component	CsCoFile_OemFiles—needed to install oem.ini file for custom VPN Clients CsCoFile_oempngFiles—needed to install icons, bitmaps, and png files		No	Yes
Directory	INSTALLDIR—Change to your own directory INSTALLDIR2—Change to your own directory Cisco_Systems_VPN_Client—Change to your own folder name		Yes for all	No for all
Feature Components	Complete | CsCoFile_OemFiles—needed to install oem.ini file for custom VPN Clients CsCoFile_oempngFiles—needed to install icons, bitmaps, and png files		No	Yes

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-15404-02
Fls. Nº 122
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 123
3698
Doc.

8535
A.

Cisco Systems

Q & A

Cisco Secure **Access Control Server** Solution Engine

Q. What is Cisco® Secure Access Control Server (ACS) Solution Engine?

A. Cisco Secure ACS Solution Engine is a highly scalable, one-rack-unit (RU), dedicated platform that serves as a high-performance access control server supporting centralized Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+). Cisco Secure ACS Solution Engine controls the authentication, authorization, and accounting (AAA) for users accessing corporate resources through the network.

Q. What does Cisco Secure ACS Solution Engine do?

A. Cisco Secure ACS Solution Engine enables you to control who can access the network, to authorize what types of network services are available for users or groups of users, and to keep an accounting record of all user actions in the network. The Solution Engine supports access control and accounting for dial-up access servers, firewalls and VPNs, voice-over-IP (VoIP) solutions, content networking, storage networks, and switched and wireless LANs (WLANs). In addition, the AAA framework can be used to manage the administrative roles and groups via TACACS+ and to control how network administrators are able to change, access, and configure the network internally.

Q. Why did Cisco add an Solution Engine to the existing Windows server software packaging for Cisco Secure ACS?

A. The decision to create a dedicated solution engine version of Cisco Secure ACS was made based on several factors:

- Security—The need to create a turnkey security-hardened service focused on running the Cisco Secure ACS service exclusively. The solution engine can remove all extraneous services, block all unused ports, and otherwise prevent all other access to the Cisco Secure ACS server system—dramatically increasing the security posture of Cisco Secure ACS.
- Manageability—Cisco Secure ACS Solution Engine is a dedicated, exclusive service for AAA with no ability to install or run other services or applications. This greatly facilitates the support and day-to-day management of the Cisco Secure ACS system.
- Reliability—By targeting only the operating system services required by Cisco Secure ACS, the solution engine offers greater operational reliability and security for the Cisco Secure ACS system.
- Total cost of ownership—Customers choosing Cisco Secure ACS can optimize their total cost of ownership. Cisco end-to-end support now includes

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 124
Doc. 3698

full support, maintenance, and serviceability of the Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations and supported by various third-party vendors.

- Plug and play—Cisco Secure ACS Solution Engine is shipped already installed with Cisco Secure ACS application software, greatly reducing the time it takes to set up and deploy Cisco Secure ACS in your network.
- Migration from Cisco Secure ACS UNIX—Cisco Secure ACS Solution Engine was built and targeted as a suitable migration platform for Cisco Secure ACS for Unix customers not willing to install or manage Cisco Secure ACS on a Windows server.

Q. What are the differences between the Cisco Secure ACS software server and Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine provides the same features and functions of the Cisco Secure ACS Windows version—in a dedicated, security-hardened, application-specific option. The appliance includes features specific to the operation and management of Cisco Secure ACS, and specific software features needed to be customized or removed due to the different underlying system architectures:

Authentication

- Authentication against a Windows domain requires a Cisco Secure ACS remote agent running on a domain controller or member server. The Cisco Secure ACS remote agent is necessary to establish a Windows member or domain controller trust relationship.
- Authentication against an Open Database Connectivity (ODBC) source is not supported. Lightweight Directory Access Protocol (LDAP) authentication can be used instead.
- Authentication against One-Time Password (OTP) directories is performed using the generic RADIUS-based OTP interface on the appliance. Any OTP vendor that provides an RFC-compliant RADIUS interface can interface with Cisco Secure ACS.

User Database Synchronization

- User database synchronization with an ODBC source is not supported. Instead, the administrator can configure Cisco Secure ACS to synchronize its user database with a comma-separated values (CSV) file on a remote File Transfer Protocol (FTP) server.

ODBC Logging

- ODBC logging is not supported. Administrators can use local or remote CSV logging.

Backup/Restore and Appliance Diagnostics

- Backup/restore and gathered appliance diagnostics are performed through a remote FTP server and configured using the current Cisco Secure ACS HTML graphical user interface (GUI).

Q. What additional features are available on Cisco Secure ACS Solution Engine but not available on the Windows version?

A. To ensure the highly secure posture of Cisco Secure ACS Solution Engine, functions specific to operating and managing the appliance have been added:

- Security-hardened underlying operating system.
- Port-based packet filtering, allowing connections only to the ports necessary for Cisco Secure ACS operation.
- Serial console interface for initial configuration, subsequent management of IP connections, Web interface, and application of upgrades and remote reboots. The serial console interface supports both serial line and Telnet connections.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 125
Doc. 3698

8533
A.

- Backup/restore of Cisco Secure ACS data via FTP protocol.
- Recovery procedures.
- NTP (Network Time Protocol) support for maintaining network time consistency with other appliances or network devices.

Q. Are there any additions to the existing Cisco Secure ACS GUI to support Cisco Secure ACS Solution Engine?

A. Yes. New HTML pages specific to Cisco Secure ACS Solution Engine have been added to the Cisco Secure ACS GUI. These pages cover specific features around the operation and management of the solution engine and include:

- Solution Engine configuration page
- Solution Engine remote agent configuration page
- Solution Engine upgrade page
- Solution Engine status page
- Solution Engine diagnostics log view

Q. What ports and protocols access Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine implements a packet filtering service to block the traffic on all but necessary TCP/User Datagram Protocol (UDP) ports. Only the ports listed in Table 1 are open for input traffic:

Table 1 Cisco Secure ACS Solution Engine Ports Usage

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication and authorization (original draft RFC)	1645	
RADIUS accounting (original draft RFC)	1646	
RADIUS authentication and authorization (revised RFC)	1812	
RADIUS accounting (revised draft RFC)	1813	
TACACS+ AAA		49
Replication and RDBMS synchronization		2000
Cisco Secure ACS remote logging		2001
Cisco Secure ACS distributed logging (appliance only)		2003
Hypertext Transfer Protocol (HTTP) administrative access (at login)		2002
Administrative access (after login) port range		Configurable (default 1024-65535)[1]

1. ACS assigns unique port number from the range to each administration session

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 126
3698
Doc.

8532
A.

Q. What is the hardware platform specification for Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine is a security-hardened Cisco Secure ACS server in a dedicated 1-RU box with the following configuration:

- Intel ISP 1100 motherboard with a 2.66-GHz Pentium 4 processor
- 1 GB of RAM
- Two built-in 10/100 Ethernet controllers
- 40-GB IDE hard drive
- One floppy drive
- One CD-ROM drive

Q. How does Cisco Secure ACS Solution Engine authenticate to Windows domains?

A. In general, to authenticate Windows NT 4.0 or Active Directory domain users, you must establish a Windows member or domain controller trust relationship. Since Cisco Secure ACS Solution Engine does not run the necessary Windows server services to establish this trust, an external Cisco Secure ACS remote agent is provided with the appliance solution, allowing the trust relationship to be established. The Cisco Secure ACS remote agent can be installed on member servers, domain controllers, or backup domain controllers. NOTE: The best practice is to install the remote agent on a full Domain Controller (DC), as this would allow it to perform its authentication functions with the least extra configuration requirements.

Q. What is the main purpose of the Cisco Secure ACS remote agent?

A. The Cisco Secure ACS remote agent has dual roles—it enables authentication against Windows domains, and it allows remote logging capabilities of user accounting records.

Q. What operating systems can the Cisco Secure ACS remote agent be installed on?

A. The Cisco Secure ACS remote agent can be installed on a Windows 2000 server (Windows Domain Controller or Member Server supported). A Solaris version of Cisco Secure ACS will be provided in the future for Sun Solaris installations. Please refer to the Cisco Secure ACS remote agent installation guide for the exact operating system versions and service packs supported.

Q. Can a Cisco Secure ACS remote agent and Cisco Secure ACS Windows coexist on the same server?

A. No. The Cisco Secure ACS remote agent cannot be installed on a server that already has Cisco Secure ACS Windows installed.

Q. Can a solution engine be configured to use several remote agents?

A. Yes. A solution engine can be configured to use one or more agents. There is no restriction that the same agent be used for Windows services and logging services. For Windows services, an appliance can point to a primary and backup agent, in the event that the primary agent is unavailable.

Q. Can a Cisco Secure ACS remote agent be shared with multiple solution engines?

A. Yes. The Cisco Secure ACS remote agent can be shared with multiple solution engines. There is no hard limit to the number of Cisco Secure ACS solution engines that can share a single remote agent, but Cisco will support configurations with up to five solution engines sharing a single Cisco Secure ACS remote agent. If user accounting records from multiple Cisco Secure ACS solution engines need to be consolidated and centralized, it is desired that all these solution engines share a single Cisco Secure ACS remote agent.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI -- CORREIOS
Fls. Nº 127
Doc. 3698

Q. Can I perform local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent?

A. Yes. However, local logging on Cisco Secure ACS Solution Engine is constrained in size, forcing log files to be recycled after seven days. The Cisco Secure ACS remote agent provides full, unconstrained logging capability to a remote server.

Q. Are there any differences in the type of Windows databases supported by the Cisco Secure ACS remote agent and the ones supported by Cisco Secure ACS Windows?

A. No The Cisco Secure ACS remote agent supports the same Windows databases supported by Cisco Secure ACS Windows

Q. What 802.1X authentication types does the Cisco Secure ACS remote agent support?

A. The Cisco Secure ACS remote agent supports the same 802.1X authentication types available on Cisco Secure ACS for Windows. This includes Extensible Authentication Protocol (EAP)-MD5, EAP-TLS, EAP Cisco Wireless, LEAP, PEAP-EAP-GTC, and PEAP-EAP-MSCHAPv2.

Q. Can a Cisco Secure ACS remote agent be provisioned for Cisco Secure ACS for Windows?

A. No. In its initial release, the Cisco Secure ACS remote agent only operates with Cisco Secure ACS Solution Engine. No communication is possible between a Cisco Secure ACS remote agent and a Cisco Secure ACS service on Windows. However, this limitation does not prevent Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine from operating in the same network environment.

Q. What happens to the standard HTML reports on the solution engine? Do they stay the same?

A. In general, these reports stay the same. The solution engine reports will be constrained in size with no support for multiple rolled over files. The Cisco Secure ACS remote agent will provide full, unconstrained report capability on a remote FTP server.

Q. What happens with third-party software tools, such as backup services from Legato?

A. Cisco Secure ACS Solution Engine is a standalone, dedicated box for running Cisco Secure ACS. There are no interfaces or abilities to add third-party software of any kind to the box. Cisco will investigate third-party extensibility, but at present, nothing can be installed on the Cisco Secure ACS Solution Engine other than Cisco Secure ACS images and patches downloaded via FTP. For Cisco Secure ACS backup, Cisco will create an export file that is automatically exported to an external FTP server. Backup tools can be installed and used to backup the external server.

Q. Can I run Cisco Secure ACS in "mixed mode" (for example, run instances of the Cisco Secure ACS Windows and additional instances of Cisco Secure ACS Solution Engine)?

A. Yes. Cisco will support environments using both Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine.

Q. How is Cisco Secure ACS replication affected with the introduction of Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS replication functions will remain unchanged with the introduction of Cisco Secure ACS Solution Engine. Replication between Cisco Secure ACS Solution Engine and Cisco Secure ACS Windows, as well as replication among Cisco Secure ACS solution engines, will be supported with no impact on any of the solution engines or Windows configurations.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 128
Doc. 3698

8530
A

Q. Are there any restrictions on whether Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be a master database in a replicated configuration?

A. No. Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be the master databases replicating to Cisco Secure ACS Windows slaves, Cisco Secure ACS Solution Engine slaves, or both Windows and solution engine slaves at the same time.

Q. Are there any changes to single logon and password aging capabilities in Cisco Secure ACS Solution Engine?

A. No. With the appropriate Windows or domain controller trust relationships established with the Cisco Secure ACS remote agent, single logon and password aging capabilities remain unchanged from Cisco Secure ACS Windows version.

Q. How scalable is a Cisco Secure ACS Solution Engine?

A. The Cisco Secure ACS Solution Engine follows, as a minimum, the same scalability performance as a Windows-based Cisco Secure ACS server. Cisco Secure ACS guidelines and performance analysis shows that each Cisco Secure ACS server can support anywhere from 20,000 to 80,000 users per server, and can scale to support in excess of 10,000 devices, depending on configuration, platform, and usage scenarios. The real challenge in scaling a user access control framework is on the back end. Linked to a high-performance back-end database such as Oracle or Sybase, Cisco has deployed Cisco Secure ACS for Windows 2000 and NT in clustered deployments into customers with hundreds of thousands of user records.

Q. What Cisco Secure ACS Solution Engine features enhance Cisco Secure ACS reliability and remote management?

A. The operating system is configured to automatically reboot on system crash. The serial console service is configured to automatically restart if it fails. Cisco Secure ACS software implements the monitor that will restart Cisco Secure ACS services if they fail. The solution engine also provides a remote administrator command line interface (CLI). The CLI supports both serial line and Telnet connections, and the Cisco Secure ACS service can be reimaged, reloaded, upgraded, and rebooted remotely from the CLI interface.

Q. What support is there for LDAP?

A. Support for LDAP on the appliance is identical to present support from the Cisco Secure ACS Software version. Cisco Secure ACS supports user authentication against records kept in a directory server through LDAP. Cisco Secure ACS supports the most popular directory servers, including Novell and Netscape LDAP Servers, through a generic LDAP interface.

Q. Will Cisco Secure ACS Solution Engine allow "single login" for Windows networking?

A. Yes. Cisco Secure ACS can be set up so that a user will only need to enter a user name and password once. This is considered a "single login." The Cisco Secure ACS remote agent is required to be installed on a Windows network server with the necessary trust relationships to the domain defined.

Q. Does Cisco Secure ACS support OTP and token systems?

A. Yes. Cisco Secure ACS can be configured to communicate with token solutions from ActiveCard, Cryptocard, PassGo Technologies, RSA Data Security, Secure Computing, and Vasco. Cisco Secure ACS Solution Engine includes a generic RADIUS interface for expanding OTP coverage to new vendors. Any OTP vendor that provides an RFC-compliant RADIUS interface should work with Cisco Secure ACS Solution Engine.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 129
Doc. 3698

8529
A

Q. What's new in Cisco Secure ACS Version 3.2 for access control functions and features?

A. Cisco Secure ACS Version 3.2 is a minor update to Cisco Secure ACS Version 3.1. It adds the following main features:

- Cisco Secure ACS Solution Engine support
- EAP-MSCHAPv2 support within the Protected EAP (PEAP) framework (used for both wireless and wired environments)
- Machine-based authentication (through EAP-TLS and EAP-MSCHAPv2)
- PEAP authentication against the internal Cisco Secure ACS database
- EAP-TLS authentication against ODBC databases
- EAP-TLS session resume support
- Accounting support for Cisco Aironet® clients
- LDAP multithreading
- Downloadable access control lists (ACLs) for VPN solutions

Please refer to the Cisco Secure ACS Version 3.2 data sheet for more information about the features and functions introduced in this release.

Q. How is Cisco Secure ACS Solution Engine Version 3.2 licensed?

A. Cisco Secure ACS Solution Engine is licensed per server, with unlimited ports, users, and network access servers. The following solution engine packages will be available for ordering. For exact part numbers, refer to the Cisco Secure ACS Version 3.2 product bulletin at: http://www.cisco.com/go/acs

- Cisco Secure ACS Solution Engine Version 3.2
- Cisco Secure ACS Solution Engine upgrade package—Used for upgrading from software versions of Cisco Secure ACS 3.x or Cisco Secure ACS for UNIX to Cisco Secure ACS Solution Engine Version 3.2

Note: The Cisco Secure ACS Solution Engine upgrade package can be ordered when customers have deployed Cisco Secure ACS for Windows or Cisco Secure ACS for UNIX in their networks and want to upgrade to the solution engine version. Please refer to the Cisco Secure ACS Solution Engine user guide and release notes for supported upgrade paths. Current Cisco Secure ACS software maintenance entitlements do not provide a free upgrade to the Cisco Secure ACS Solution Engine.

Q. Can I upgrade to Cisco Secure ACS Version 3.2 from older software versions of Cisco Secure ACS?

A. Yes. A detailed upgrade procedure will be available to guide you through the required steps to complete an upgrade to Cisco Secure ACS Solution Engine. Please refer to the Cisco Secure ACS Solution Engine user guide for more information about the supported upgrade procedure.

Q. Can I purchase or license a backup solution engine?

A. No. An additional Cisco Secure ACS Solution Engine must be purchased as a separate Cisco Secure ACS server license to be used for recovery and backup purposes. Cisco Secure ACS servers can be run as recovery or failover servers. Because Cisco Secure ACS is a central control service in your network, Cisco highly recommends that customers configure a backup server for failover and recovery.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 130
Doc. 3698

8528
A.

Q. Does Cisco Secure ACS Solution Engine operating system need to be updated when upgrading the Cisco Secure ACS firmware?

A. No. Future Cisco Secure ACS image upgrades are applied to Cisco Secure ACS Solution Engine without updating or modifying the underlying Cisco Secure ACS Solution Engine operating system.

Q. Do I need to patch the solution engine with newer operating system releases or patches?

A. No. All operating system software updates and patches are handled by Cisco Secure ACS Solution Engine upgrades performed by Cisco. Any operating system patch that requires changes to Cisco Secure ACS Solution Engine will be provided in a new upgrade/patch.

Q. Can Cisco Secure ACS Solution Engine software be upgraded remotely from a CD-ROM?

A. Yes. Cisco Secure ACS Solution Engine supports remote upgrades from CD-ROM without any FTP server posting requirements.

Q. Can Cisco Secure ACS Solution Engine support software image rollback during patch update verification?

A. Yes. Cisco Secure ACS Solution Engine can roll back to previously installed software when a software patch has been applied. This capability is used for debugging and verification purposes.

Q. What is the status of Cisco Secure ACS for UNIX?

A. Cisco Secure ACS for UNIX is expected to be discontinued, at which point an end-of-life, end-of-sale (EOL/EOS) announcement will be made. Cisco will support all existing customers and provide smooth migration paths as the new platforms become available. The EOL/EOS date has not been determined, but Cisco will provide customer support for Cisco Secure ACS for UNIX customers for a period no shorter than 24 months after the EOL/EOS date. At present, no new features or releases are planned for Cisco Secure ACS for UNIX and only critical, Priority 1 bugs will be addressed.

Q. Can I use my current Cisco Secure ACS Windows maintenance contract to get support on Cisco Secure ACS Solution Engine?

A. No. Separate hardware and software contracts need to be purchased for maintenance support on Cisco Secure ACS Solution Engine. Please refer to refer to the Cisco Secure ACS Version 3.2 product bulletin for more information. http:// www.cisco.com/go/acs

Q. How can I obtain a demo of Cisco Secure ACS Solution Engine?

A. Please contact your Cisco account manager, who will be able to arrange for a limited time demo of Cisco Secure ACS Solution Engine.

Q. Where can I find more information on Cisco Secure ACS?

A. For additional product information, visit: http://www.cisco.com/go/acs

For additional information or questions, please send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 131
Doc. 3698

8527
A-

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Aironet are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203051/ETMC 05/03

RUBRICA - 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 132
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 133
Doc. 3698

Cisco Secure Access Control Server v3.2 for Windows

Product Overview

The Cisco Secure Access Control Server (ACS) provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure. The Cisco Secure ACS is a highly scalable, high performance access control server that operates as a centralized Remote Access Dial-In User Service (RADIUS) server or TACACS+ server. It extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking solution, allowing for greater flexibility and mobility, increased security, and user productivity gains.

Cisco Secure ACS Version 3.2 allows network administrators to control:

- Who can log into the network from wired or wireless connections
- What privileges each user has in the network
- What accounting information is recorded in terms of security audits or account billing
- What access and command controls are enabled for each configuration administrator

Key Features and Benefits

Cisco Secure ACS Key New Features

- Protected Extensible Authentication Protocol (PEAP) support for Microsoft® Windows and Cisco clients—Provides support for Microsoft® PEAP on Windows 98, NT, 2000 and XP by supporting client authentication with MS-CHAPv2, and support for Cisco PEAP with one-time token authentication and support of non-MSCHAP end-user databases such as LDAP, NDS, and ODBC.
- EAP mixed configurations—Allows flexible EAP settings to be set concurrently and processed per the 802.1X protocol presented by the end user. ACS supports PEAP-EAP-GTC (Cisco PEAP), PEAP-EAP-MSCHAPv2 (Microsoft® PEAP), EAP-TLS, EAP-MD5, and Cisco EAP Wireless (LEAP).
- EAP-TLS enhancements—Extends ACS PKI capabilities with the addition of EAP-TLS authentication against ODBC user databases, and EAP-TLS silent session resume support which prevents users from re-authenticating during a RADIUS session timeout.
- Machine authentication support—Supports machine authentication by maintaining communication to a back end Windows Active Directory during boot time. ACS supports machine authentication using PEAP with MSCHAPv2 or EAP-TLS 802.1X authentication types.
- LDAP Multithreading—Increases performance by processing multiple LDAP authentication requests in parallel rather than in sequential order.
- Accounting Support for Aironet—Supports user-based accounting from the Aironet Wireless Access Points when they are configured as RADIUS (Cisco Aironet) AAA clients.
- Downloadable access control lists for Virtual Private Network (VPN) users—Allows administrators to define access control lists of any length, per user or group of users. It extends per-user access control list support to Cisco VPN solutions and PIX Firewall solutions.

Cisco Secure ACS Benefits

Cisco Secure ACS is a powerful access control server with many high-performance and scalability features for any organization growing its WAN or LAN connectivity:

- Ease of use—A Web-based user interface simplifies and distributes configuration for user profiles, group profiles, and Cisco Secure ACS configuration.

RQS nº 03/2005 - CN
CRMV - CORREIOS
Fls. Nº 134
Doc. 3698

- Scalability—Cisco Secure ACS is built to support large networked environments with support for redundant servers, remote databases, and user database backup services.
- Extensibility—LDAP authentication forwarding supports the authentication of user profiles stored in directories from leading directory vendors such as Netscape, Novell, and Microsoft.
- Management—Windows Active Directory and NT database support consolidates Windows username/password management, and utilizes the Windows Performance Monitor for real-time statistics viewing.
- Administration—Different access levels for each Cisco Secure administrator-and the ability to group network devices-enables easier control and maximum flexibility to facilitate enforcement and changes of security policies administration over all the devices in a network.
- Product flexibility—Because Cisco IOS® Software has embedded support for AAA, Cisco Secure ACS can be used across virtually any NAS that Cisco sells. (The Cisco IOS version must support RADIUS or TACACS+.)
- Protocol flexibility—Cisco Secure ACS includes simultaneous TACACS+ and RADIUS support for a flexible solution with VPN or dial support at the origin and termination of Internet Protocol Security (IPSec) and Point-to-Point Tunneling Protocol (PPTP) tunnels.
- Integration—Tight coupling with Cisco IOS routers and VPN solutions provides features such as Multi-chassis Multilink Point-to-Point Protocol and Cisco IOS command authorization.
- Third-party support—Cisco Secure ACS offers token server support for any one-time password (OTP) vendor that provides an RFC-compliant RADIUS interface (Rivest, Shamir, Adelman [RSA] SecurID, Passgo, Secure Computing, ActiveCard, Vasco, and CryptoCard).
- Control—Cisco Secure ACS provides dynamic quotas for time-of-day, network usage, number of logged sessions, and day-of-week access restrictions.

Specifications

Table 20-8: System Specifications for Cisco Secure ACS 3.2 for Windows

Description	Specification
Hardware	Intel class Pentium 550 MHz PC or compatible 256 MB of RAM 250 MB of free disk space; more if you are running your database on the same device Minimum resolution of 256 colors at 800 x 600
Software	English-language version of Windows 2000 Server Microsoft Internet Explorer 5.5 or 6.0 Netscape Communicator 6.2

Ordering Information

Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at

http://www.cisco.com/cgi-bin/front.x/pricing

The Cisco Pricing tool requires a username and password. If you are not already registered, go to

http://www.cisco.com/register and follow the instructions. After you have registered, you may access the pricing tool.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 135
3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 136
Doc. 3699

CISCO SYSTEMS

8524
A-

Q & A

Cisco **Secure Policy Manager** Version 3.1

Q. What are the new features of CSPM 3.1?

A. New features of CSPM 3.1 include the following:

- Windows 2000 Server
- Windows 2000 Workstation
- Improved client/server
- Network object comment
- Cisco IOS Software releases 12.1(10),12.1(11),12.1(8)E, 12.1(9)E, 12.1(10)E,12.2(5),12.2(4)T
- Database enhancements

Q. What are the key features and benefits of Cisco Secure Policy Manager?

A. CSPM's main features and benefits are as follows:

- *Cisco firewall management*—Easily defines perimeter security policies for Cisco Secure PIX Firewalls and Cisco IOS routers running the firewall feature set.
- *Cisco VPN router management*—Easily configures intranet/extranet IPSec VPNs based on Cisco PIX Firewalls and Cisco's suite of VPN routers running the Cisco IOS IPSec software.
- *Security policy management*—Uses network-wide policies to manage Cisco security devices without requiring extensive device knowledge and dependency on the command-line interface (CLI).
- *Notification and reporting system*—Provides basic auditing tools to monitor, alert, and report Cisco security device and policy activity, thereby keeping the network administrator readily informed of network-wide events. CSPM also complements and interoperates with third-party monitoring, billing, and reporting systems.
- *Windows 2000-based system*—Provides an easy-to-use Windows-based user interface
- *Network operations*—CSPM incorporates many network operational features including topology import from CiscoWorks, CLI policy mapping, command diff, admin password aging, and policy query.

Q. Is CSPM part of CiscoWorks?

A. Yes. CSPM 3.1 is available exclusively in CiscoWorks VPN/Security Management Solution (VMS).

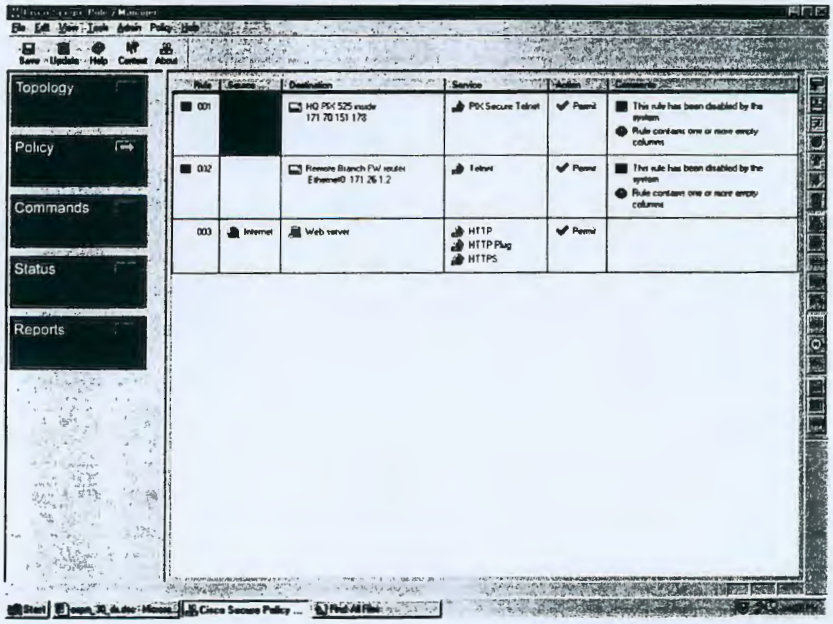
Q. Does CSPM 3.1 have a similar "look and feel" to that of the Cisco PIX Device Manager (PDM)?

A. Yes. CSPM 3.1 includes a rule table that is similar to that of Cisco PDM. Customers that are familiar with PDM can migrate easily to CSPM, which has a similar interface. The following graphic is an example of the CSPM 3.1 rule table.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 137
Doc. 3698

8523
A.



Q. Can CSPM 3.1 import security configuration files generated by Cisco PDM?

A. Yes. CSPM offers a configuration import tool. This import tool will create and end-to-end global topology of the Cisco PIX and Cisco IOS security network. The configuration import tool will also populate the rule table with the existing security policies configured on the PIX and IOS devices. Because configuration import works on the CLI it does not matter how that CLI was created. CSPM imports security policies from any Cisco PIX Firewall or Cisco IOS router regardless of how the configuration file was originally created.

Q. Does CSPM support the Hot Standby Routing Protocol (HSRP) and multihomed servers?

A. Yes. CSPM introduces an install-on feature in the rule table for multipath networks.

Q. Will CSPM manage the access lists on a Cisco IOS device even if the firewall feature set (CBAC) is not installed?

A. Yes. CSPM 3.1 supports native access lists on Cisco IOS Software products. CSPM manages end-to-end security policies in any Cisco network.

Q. Does CSPM allow a comment for each rule?

A. Yes. CSPM 3.1 supports a comment field for each entry in the rule table.

Q. Does CSPM support network object groups and service bundles?

A. Yes. CSPM greatly simplifies security policy configuration by aggregating common networks and service protocols into network object and service bundles. Network object groups and services bundles can be used and reused in source, destination, and service fields in the rule table.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 138
Doc. 3698

8522
A.

Q. Will CSPM manage Cisco IOS Software images on the Cisco Catalyst® product line?

A. No. CSPM does not support the Cisco Catalyst product line. The Router Management Center in CiscoWorks VMS and access control list (ACL) management in CiscoWorks Routed WAN Management Solution (RWAN) support the Cisco Catalyst product line.

Q. What does CSPM manage on a firewall?

A. CSPM creates the configuration file for each Cisco firewall within a network. CSPM can also monitor syslogs and generate reports for each Cisco firewall.

Q. What does CSPM manage on a VPN router?

A. CSPM creates configuration files for hub-and-spoke as well as meshed site-to-site VPN routers.

CSPM is an excellent choice for centralized management of remote VPN devices while abstracting the Crypto-map and Certificate Authority complexities of VPNs.

CSPM can also monitor syslogs and generate reports for VPN routers.

Q. What is policy-based management, and how does Cisco Secure Policy Manager support it?

A. A policy is a set of high-level business directives that control the deployment of network services. Customers typically establish network policies within their organizations on the basis of established business practices. These policies involve the control of various services such as network availability, performance, and security. The creation, maintenance, and auditing of these policies are essential in order for the organization and its network to operate effectively.

Policy-based management is the overall process by which organizations administer these policies. In general, policy-based management encompasses three basic processes:

- *Policy definition*—Policy includes the creation of network security policies. For example, a network security policy might be to "allow all members of the Engineering department to browse the Web and download files via FTP."
- *Policy enforcement*—Policy enforcement means the automatic translation, validation, and distribution of the defined network security policies. Translation is required so that policies that are independent of the underlying network devices and topology may be constructed. Validation is necessary to ensure that defined network security policies and the resultant configurations do not conflict with one another or with various devices within the network. This process also ensures the distribution of policies to the appropriate network(s).
- *Policy auditing*—Policy auditing involves the logging, monitoring, and reporting on the status of policies within the network and critical network events. Logging provides a basis for accountability for all device, policy, and user actions on the network. Monitoring of these actions is useful to determine when the network is not being used in accordance with the established network security policies. The reporting function allows a network security administrator to examine actions and events that have occurred on the network.

Cisco Secure Policy Manager provides a level of management abstraction between the administrator and the network devices. This layering provides a translation between high-level policies developed for business purposes and the implementation of these policies, in the form of device configurations, within the network. This setup simplifies and organizes the task of consistently enforcing security policy throughout large, distributed networks.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
OPMI - CORREIOS
Fls. Nº 139
Doc. 3698

8521
A.

Q. What devices can Cisco Secure Policy Manager administer within a network?

A. CSPM 3.1 provides policy-based administration of Cisco PIX firewalls as well as Cisco IOS firewalls, VPN routers running the firewall features. More specifically, CSPM 3.1 supports the following devices and software versions:

Platform	Software Version Supported
Cisco PIX Firewall	4.2.4
	4.2.5
	4.4.x
	5.1.2
	5.2.1
	5.3.x
	6.0.x
	6.1.x
Cisco IOS router	12.0(5)T, 12.0(5)XE5
	12.0(7)T
	12.1(1), 12.1(1)T, 12.1(1)E, 12.1(1)XC
	12.1(2), 12.1(2)T, 12.1(2)XH
	12.1(3), 12.1(3)T, 12.1(3)XI
	12.1(4), 12.1(4)T, 12.1(4)E
	12.1(5), 12.1(5)T
	12.1(6), 12.1(6)E,
	12.1(7), 12.1(7)E, 12.1(8),
	12.1(9), 12.2(1), 12.2(2)T,
	12.1(10), 12.1(11),12.1(8)E, 12.1(9)E, 12.1(10)E,12.2(5),12.2(4)T, 12.2(3)

1. Cisco IOS IDS and Cisco PIX IDS are not supported.

Q. Does CSPM support Cisco PIX Firewall Version 6.2?

A. No. Cisco PIX Firewall Version 6.2 is supported by the CiscoWorks Management Center for PIX Firewalls.

Q. Why is IDS not supported in CSPM?

A. The award-winning alarm event viewer in CSPM has been incorporated into Cisco's next-generation IDS management platform. This next-generation platform, CiscoWorks Management Center for IDS, is available with CSPM in CiscoWorks VMS.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 140
3698
Doc.

Q. How does CSPM 3.1 improve the client/server model?

A. CSPM 3.1 implements the client/server model with Microsoft Terminal Services. Leveraging an optimized, thin client/server solution allows CSPM client users to enjoy greater throughput, reduces latency and more client platform options.

Q. Does CSPM 3.1 offer a lite, or restricted, device license version?

A. Yes. CSPM 3.1 is a featured component of the CiscoWorks VMS solutions bundle. The VMS bundle contains a restricted 20-device option. A Cisco PIX failover bundle appears as a single device to CSPM.

Q. What network topologies does Cisco Secure Policy Manager effectively manage?

A. CSPM supports Cisco firewall and VPN router deployments within Internet, intranet, and extranet topologies. For VPN environments, the product supports site-to-site (that is, router-to- router) network topologies only. Remote access (that is, client-to-router) VPN networks are not supported.

Q. Does Cisco Secure Policy Manager offer user-based security policy management?

A. No, CSPM does not currently provide comprehensive management of user policies (for example, user-based authentication and authorization). However, because Cisco firewalls and routers provide authentication, authorization, and accounting (AAA) support for its users by linking into a Cisco Secure server, CSPM will allow the network administrator to configure these user policies through a simple command interface.

Q. Does Cisco Secure Policy Manager provide secure remote management support?

A. Yes, CSPM supports secure remote management of Cisco PIX firewalls and Cisco routers that support firewall and VPN capabilities. The CSPM product uses an embedded IPSec solution for secure configuration distribution.

Q. Does CSPM offer any offline configuration capabilities?

A. Yes, CSPM allows a security administrator to configure network security policies without requiring connectivity to a "live," complete, and established network. With the powerful, policy translation functionality of the product, device configurations can be easily and quickly generated for multiple security devices within the network. This process helps IS organizations in staging their networks for new device deployment. CSPM can then be used to distribute these configurations to the appropriate devices—or the generated configuration files can be exported and distributed to the devices via other methods, such as Trivial File Transfer Protocol (TFTP).

Cisco Secure Policy Manager also has the powerful ability to export the network topology, policy definitions and device configurations to a .cpm file. This .cpm file can be imported to another copy of CSPM which allows easy interaction with the Cisco Technical Assistance Center (TAC) and other support networks.

Q. Can Cisco Secure Policy Manager configure authentication services on Cisco firewalls and VPN routers?

A. Yes, within VPN environments, the product can configure devices to support either preshared keys or support certificates provided by a certificate authority (CA). CSPM supports authentication services such as TACACS+ or Remote Access Dial-In User Service (RADIUS) within its policy interface.

Q. Can the network data gathered by Cisco Secure Policy Manager be exported to other applications?

A. Yes, CSPM manages different types of data, and some of this gathered data can be exported. The ability to export the data depends on its data type. The following types of data can be exported:

- *Device file configurations*—The router and firewall file configurations created as a result of applying policies in the network can be exported and saved in ASCII text format.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 141
3698
Doc.

8519
A.

- *Audit event data*—All auditing data collected and stored within the Cisco Secure Policy Manager system may be exported into an ASCII text file on the local machine. Additionally, the system may be configured to dump (or permanently export) all log audit events into an Open Database Connectivity (ODBC)-compliant database.
- *Policy configurations*—The network topology and policy configuration data contained within the entire policy management system can be saved and exported. This capability allows customers to save and export their policy configurations to other Cisco Secure Policy Manager consoles within their networks, thus reducing configuration time and effort. It also enables customers to send their policy system configurations to a Cisco TAC for troubleshooting and problem resolution.
- *Topology information*—Network topology can be exported in .xml file format.

Q. Can I use Cisco Secure Policy Manager to configure my existing Cisco routers and Cisco PIX firewalls?

A. Yes, Cisco Secure Policy Manager enables a network administrator to manage existing Cisco security devices throughout the network. The existing Cisco devices within the network must be manually added to the CSPM system prior to defining and distributing policies to them. Using built-in CSPM "wizards" simplifies and expedites this process.

Upon defining policies with Cisco Secure Policy Manager, the system provides the network administrator with the capability to verify specific device configuration changes needed to enforce the defined policies. This level of verification provides the necessary device configuration details prior to policy distribution and device configuration within the network.

Q. Does Cisco Secure Policy Manager offer any reporting capabilities on the security status of my network?

A. Yes, Cisco Secure Policy Manager provides Web-based reports in graph and text format on the status of security policies and security events within the network. These reports are quite basic and are generally based upon filtered syslog messages received from the managed devices. The reports included in the product include the following:

- Policy posture (that is, "what policies are applied to the devices?")
- Device status
- Top FTP sites
- Top Web sites
- Top users*
- User activity summary*
- User activity details*
- Network service summary
- Network service details
- Event summary
- Event details

* User reports are based on IP address.

Additionally, several partner applications support Cisco network security devices and provide enhanced auditing and reporting capabilities. These third-party applications include Private-I by Open System Solutions (OSS), Telemate.Net by Telemate, and netForensics by NetCom Systems.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 142
Doc 3698

8518
A.

Q. Are there different administrator levels within Cisco Secure Policy Manager?

A. Yes, the product provides three levels of administration:

- *Full access*—This level provides read and write access to all policy administration functions within CSPM. This level also allows the user to create other administrator accounts. This level would be appropriate for the network security administrator within a company or department. Only a single network security administrator can have full access rights to the system at any one time.
- *Read only*—This level provides read-only access to all policy administration functions within CSPM. This level would be appropriate for help-desk personnel or a network security administrator with auditing responsibilities.
- *Report viewing*— This level provides read-only access to the Web-based reports created with Cisco Secure Policy Manager. This level is appropriate for help-desk personnel or interested managers within the IS staff.

Additional administration levels based on functional roles and domain responsibilities will be added in a future product release.

Q. On what operating systems does Cisco Secure Policy Manager run?

A. Cisco Secure Policy Manager 3.1 runs on Windows 2000 Server and Workstation.

Cisco Secure Policy Manager also features a client/server mode—in which the graphical user interface (GUI) resides on a separate host than the policy server function - the operating system support is as follows:

- The policy server component must run on a Windows 2000 Server or Workstation with Service Pack 2
- The policy administrator component (that is, the GUI) can run on any platform supported by Windows Terminal Services

Q. Does Cisco Secure Policy Manager offer any Web browser-based applications?

A. Yes, CSPM provides Web browser-based reports that are accessible using the following Internet browsers:

- Microsoft Internet Explorer 5.5, 6.0
- Netscape Navigator 4.75, 4.77, 4.78

Secure access to the reports within CSPM is also provided via Secure Socket Layer (SSL).

Q. Can I use my existing Microsoft or Netscape Web server to run the reports within Cisco Secure Policy Manager?

A. No, the Web-based reports within CSPM are currently supported only by the Web server embedded within the policy management system.

Q. Does Cisco Secure Policy Manager use a database?

A. Yes, CSPM uses a proprietary object-oriented database that has been optimized and secured for use in the policy-based management system. The object schema employed within this database is consistent with the work being done within the Directory-Enabled Networks (DEN) initiative.

Q. Does Cisco Secure Policy Manager integrate with any directory services?

A. No, CSPM does not currently integrate with any network directories. The Cisco Secure Access Control Server (ACS) does offer a Lightweight Directory Access Protocol (LDAP) proxy, and future product releases will further integrate with Cisco ACSs and support network directories in order to provide enhanced policy management.

Q. Does Cisco Secure Policy Manager integrate with any third-party network management systems (NMS)?

A. Yes, CSPM allows syslog forwarding to other NMS stations.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT/ECS nº 03/2005 - CN
CPMI - CORREIOS
143
Fls. Nº
3698
Doc.

Q. Does Cisco Secure Policy Manager interoperate with any CA servers?

A. Yes, CSPM supports CA servers within a VPN network. CA servers can be added to the network topology so that Cisco devices can identify and communicate with them to acquire a certificate for authentication purposes. Certificate information such as owner, signing authority, serial number, and supported time frame can be "discovered" for each supported device.

CSPM interoperates with, and has been tested with, Entrust, Verisign, and Netscape CA servers.

Q. Does Cisco Secure Policy Manager support any industry standards?

A. Yes, CSPM supports several industry standards, including:

- IPSec—for secure management communications to Cisco devices (additionally, CSPM can configure IPSec VPN tunnels between firewalls and routers throughout a network)
- SSL—for secure access to the product Web-based reports
- Microsoft's Cryptography application programming interfaces (APIs) for secure communications between policy servers and policy administrators
- Syslog—for event notification and logging

Cisco is committed to open standards, and future releases of Cisco Secure Policy Manager will support additional industry standards, as appropriate.

Q. What are the system requirements for Cisco Secure Policy Manager 3.1?

A. The system requirements for CSPM are as follows:

Recommended Hardware

- Intel-based Pentium II processor, 800 MHz or better
- 1 GB RAM
- 4 GB or more free hard drive space available
- One or more properly configured network adapters
- Video display—1024 x 768, with 64k color support
- CD-ROM and 3.5-in. diskette drive

Required Software

- Microsoft Windows 2000 Server or Workstation with Service Pack 2
- Microsoft Internet Explorer 5.5, 6.0

Q. Can I upgrade to Cisco Secure Policy Manager 3.1 from any Cisco products?

A. Yes. Customers who purchased Cisco Secure Policy Manager 2.0 UR can upgrade to CiscoWorks VMS with Cisco Secure Policy Manager 3.1 and other components including Cisco Resource Manager Essentials (RME), Host IDS, and VPN Monitor for a reduced price.

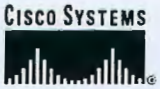
Q. Where can I get more information on Cisco Secure Policy Manager?

A. For more information on Cisco Secure Policy Manager, contact your local Cisco sales representative. You can also find additional product information at http://www.cisco.com/go/policymanager. Also, you can get more information on VMS at: www.cisco.com/go/vms

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 144
Doc. 3698

8516
A.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 119
3698
Doc.

Apêndice IIA

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 146
3698
Doc.

8515
A

Data Sheet

Cisco **VPN 3000** Series Concentrator

Introduction

The Cisco® VPN Series 3000 Concentrator allow corporations to take full advantage of the unprecedented cost savings, flexibility, performance, and reliability of remote access VPN connections. Corporations use VPNs to establish secure, end-to-end private network connections over a public networking infrastructure. VPNs have become the logical solution for remote-access connectivity for two main reasons:

• Deploying a remote-access VPN enables corporations to reduce communications expenses by using the local dialup infrastructures of Internet service providers.

• Remote Access VPNs allow mobile workers, telecommuters and day extenders to take advantage of broadband connectivity.

To fully realize the benefits of high-performance, remote-access VPNs, a corporation must deploy a robust, highly available VPN solution, and dedicated VPN devices are optimal for this purpose.

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution for enterprise-class deployment. A standards-based, asy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote access VPNs. Incorporating the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications.

Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP/SEP-E) modules, enable users to easily add capacity and throughput.

The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, the Microsoft Windows 2000/XP L2TP/IPsec Client, the Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium (ME), Windows NT Workstation 4.0, and Microsoft PPTP.

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 147
3698
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

.8514
A

Five Models

The Cisco VPN 3000 Concentrator is available in five different models:

Cisco VPN 3005 Concentrator

The Cisco VPN 3005 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Encryption processing is performed in software. The Cisco VPN 3005 does not have built-in upgrade capability.

Cisco VPN 3015 Concentrator

The Cisco VPN 3015 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Like the Cisco VPN 3005, encryption processing is performed in software, but the Cisco VPN 3015 is also field-upgradable to the Cisco VPN 3030 and 3060 models.

Cisco VPN 3030 Concentrator

The Cisco VPN 3030 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3(50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 is field-upgradeable to the Cisco VPN 3060. Redundant and nonredundant configurations are available.

Cisco VPN 3060 Concentrator

The Cisco VPN 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and nonredundant configurations are available.

Cisco VPN 3080 Concentrator

The Cisco VPN 3080 Concentrator is optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous remote access sessions. Specialized SEP modules perform hardware-based acceleration. The VPN 3080 is available in a fully redundant configuration only.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 148
3698
Doc.

8313
A.

Models Comparison

Table 1 The Cisco VPN 3000 Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous Users[1]	100	100	1,500	5,000	10,000
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Available Expansion Slots	0	4	3	2	2
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	–	–	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

1. For planning purposes, a simultaneous user is considered to be a remote access VPN user connected in all tunneling mode—this includes one IKE Security Association and two unidirectional IPsec SAs (Security Associations). For environments with rekeying or split tunneling, we recommend using a VPN remote access load-balancing environment with spare capacity because these particular sessions will use additional system resources that otherwise would be used to support additional users. The Cisco VPN 3000 Series Concentrator supports the entire range of enterprise applications.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator. This thin design, IPsec-compliant implementation is provided with the Cisco VPN 3000 Concentrator and is licensed for an unlimited number of users. The client can be pre-configured for mass deployments and the initial logons require very little user intervention. VPN access policies are created and stored centrally in the Cisco VPN 3000 Concentrator and pushed to the client when a connection is established.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 149
Doc. 3698

8512
A.

Features and Benefits

Product Highlights

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (Cisco VPN 3030–3080).
- Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPsec connections.

Scalability (Cisco VPN 3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
- System architecture is designed to supply consistent, high-availability performance.
- All digital design provides the highest reliability and 24-hour continuous operation.
- Robust instrumentation package provides run-time monitoring and alerts.
- Microsoft compatibility offers large-scale client deployment and smooth integration with related systems.

Security

- Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.
- Firewall capabilities through stateless packet filtering and address translation to ensure the required security of a corporate LAN.
- User and group level management offers maximum flexibility.

High Availability

- Redundant subsystems and multichassis failover capabilities ensure maximum system uptime.
- Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, SSHv1, and using a console port. Files can be accessed through HTTPS, FTP, and SSH Copy (SCP).
- Configuration and monitoring capability is provided for both the enterprise and the service provider.
- Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies. For larger scale deployments, the VPN 3000 Concentrators are supported in several Cisco network management applications. Those applications include:
  - *IP Solution Center (ISC)*—Provisions site-to-site and remote access VPN services
  - *VPN Monitor*—Monitors and reports on remote access and site-to-site VPN tunnel connections
  - *Resource Manager Essentials (RME)*—Provides operational management features such as software distribution, syslog reporting, inventory management
  - *CiscoView*—Provides real time system status monitoring

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 150
Doc. 3698

8511
A-

Technical Specifications

Hardware

Processor

- Motorola PowerPC Processor

Memory

- Redundant system images (Flash)
- Variable memory options (see chart)

Encryption

- *Cisco VPN 3005, 3015*—Software encryption
- *Cisco VPN 3030–3080*—Hardware encryption

Embedded LAN Interfaces

- *Cisco VPN 3005*—Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted)
- *Cisco VPN 3015–3080*—Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted and DMZ)

Instrumentation

- *Cisco VPN 3005 Front panel*—Unit status indicator
- *Cisco VPN 3005 Rear panel*—Status LEDs for Ethernet ports
- *Cisco VPN 3015-3080 Front panel*—Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan
- *Cisco VPN 3015–3080 Rear panel*—Status LEDs for Ethernet modules, expansion modules, power supplies
- *Cisco VPN 3015–3080*—Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Software

Client Software Compatibility

- Cisco VPN Client (IPsec) for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit), and Mac OS X 10.2 (Jaguar), including centralized split-tunneling control and data compression
- Microsoft PPTP/MPPE/MPPC, MSCHAPv1/v2, EAP/ RADIUS pass-through for EAP/TLS and EAP/GTC support
- Microsoft L2TP/IPsec forWindows 2000/XP (including XP DHCP option for route population)
- Microsoft L2TP/IPsec for Windows 98, Windows Millennium (ME), and Windows NT Workstation 4.0
- MovianVPN (Certicom) Handheld VPN Client with ECC
- Netlock (Mac OS 8 & 9) VPN Client

Tunneling Protocols

- IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with auto-detection and fragmentation avoidance), IPsec/TCP
- Support for Easy VPN (client and network extension mode)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 151
Doc. 3698

8500 A-

Encryption/Authentication

- IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128, 192, 256-bit) with MD5 or SHA, MPPE using 40/128-bit RC4

Key Management

- Internet Key Exchange (IKE)
- Diffie-Hellman (DH) Groups 1, 2, 5, 7 (ECDH)

Routing

- RIP, RIP2, OSPF, RRI (Reverse Route Injection), static, automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
- IPsec fragmentation policiy control, including support for Path MTU Discovery (PMTUD)
- Interface MTU control

Third-Party Compatibility

- Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Macintosh and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, SA Keon

High Availability

- VRRP protocol for multi-chassis redundancy and fail-over
- Remote Access Load Balancing clusters
- Destination pooling for client-based fail-over and connection re-establishment
- Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015–3080)

Management

Configuration

- Embedded management interface is accessible through console port, Telnet, SSHv1, and Secure HTTP (HTTPS)
- Administrator access is configurable for five levels of authorization. Authentication can be performed externally through TACACS+
- Role-based management policy separates functions for service provider and end-user management

Monitoring

- Event logging and notification through e-mail (SMTP)
- Automatic FTP backup of event logs
- SNMP MIB-II support
- Configurable SNMP traps
- Syslog output
- System status
- Session data (including client assign IP, encryption type connection duration, client OS, version, etc)
- General statistics

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 152
Doc. 3698

8509
A.

Security

Authentication and Accounting Servers

- Support for redundant external authentication servers:
  - RADIUS
  - Kerberos/Active Directory authentication
  - Microsoft NT Domain authentication
  - Microsoft NT Domain authentication with Password Expiration (MSCHAPv2)

RSA Security Dynamics (SecurID Ready), including native support for RSA 5 (Load Balancing, Resiliency)

- User authorization through LDAP or RADIUS
- Internal Authentication server for up to 100 users
- X.509v3 digital certificates (including CRL/LDAP and CRL/HTTP, CRL Caching and Backup CRL Distribution Point support)
- RADIUS accounting
- TACACS+ Administrative user authentication

Internet-Based Packet Filtering

- Source and destination IP address
- Port and protocol type
- Fragment protection
- FTP session filtering
- Site-to-Site Filters and NAT (for overlapping address space)

Policy Management

- By individual user or group
  - Filter profiles (defined internally or externally)
  - Idle and maximum session timeouts
  - Time and day access control
  - Tunneling protocol and security authorization profiles
  - IP Pool
  - Authentication Servers

Certification

- FIPS 140-2 Level 2 (3.6) in process, FIPS 140-1 Level 2 (3.1), VPNC

Ports

- Console port-Asynchronous serial (DB-9)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 153
Doc. 3698

8508
A

Table 2 Physical Characteristics

Concentrator	Cisco VPN 3005	CiscoVPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Height	1.75" (4.45cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)
Width	17.5" (44.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)
Depth	11.5" (29.21cm)	–	–	–	–
Unit without front bezel or SEPS/PS	–	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)
Unit with front bezel, no SEPS/PS	–	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)
Unit with front bezel and SEPS/PS	–	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)
Weight	8.5 lbs(3.9kg)	27 lbs(12.3kg)	28 lbs(12.7kg)	33 lbs(15kg)	33 lbs(15kg)

Table 3 Power Type and Requirements

Concentrator	Cisco VPN 3005	CiscoVPN 3015-3080
Nominal	15 watts (51.22BTU/hr)	35 watts (119.50BTU/hr)
Maximum	25 watts (85.36BTU/hr)	50 watts (170.72BTU/hr)
Input Voltage	100-240VAC	100-240VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

Environmental

- Temperature: 32 to 131 F (0 to 55 C) operating; –4 to 176 F (–40 to 70 C) nonoperating
- Humidity: 0 to 95 percent noncondensing

Regulatory Compliance

- CE Marking

Safety

- UL 1950, CSA

EMC

- FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN50082-1, AS/NZS 3548 Class A, VCCI Class A

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 154
Doc: 3698

8507
A

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW4512 0403

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 156
Doc. 3698

8506
OVERVIEW
A.

Cisco VPN 3000 Series Concentrator

A Remote Access VPN Solution

Introduction

The Cisco VPN 3000 Series Concentrator is a family of purpose-built, remote-access Virtual Private Network (VPN) platforms and client software that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today.

With the Cisco VPN 3000 Series Concentrator, customers can take advantage of the latest VPN technology to vastly reduce their communications expenditures. Unique to the industry, it is the only scalable platform to offer field-swappable and customer-upgradeable components. These components, called Scalable Encryption Processing (SEP) modules, enable users to easily add capacity and throughput.

Cisco customers can choose from a range of VPN 3000 Concentrator models, the specific unit that most suits their needs and applications. The VPN 3000 Series Concentrator includes models to support a range of enterprise customers, from small businesses with 100 or fewer remote-access users to large organizations with up to 10,000 simultaneous remote users. With all versions of the Cisco VPN 3000 Concentrator, the Cisco VPN Client is provided at no additional charge and includes unlimited distribution licensing.

The Cisco VPN 3000 Series Concentrator is available in both non-redundant and redundant configurations, allowing customers to build the most robust, reliable and cost-effective networks possible. In addition, advanced routing capabilities, such as OSPF, RIP, and Network Address Translation (NAT) are available.

Product Highlights

The Cisco VPN 3000 Series Concentrator upports a wide range of Cisco customer applications in both small- and large-sized enterprise network environments.

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, which ensures consistent performance throughout the rated capacity (3030–3080)
- Large-scale tunneling support for IPsec, PPTP and L2TP/IPsec connections

Scalability (3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path (3015–3060)
- System architecture designed to supply consistent, high-availability performance (3015–3080)
- All digital design, which provides the highest reliability and 24-hour continuous operation (3015–3080)

Copyright © 2001 Cisco Systems, Inc. All Rights Reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 157
3698
Doc.

8503
A.

- Robust instrumentation package for run-time monitoring and alerts (3015–3080)
- Microsoft® compatibility, which offers large-scale client deployment and seamless integration with related systems (3015–3060)

Security

- Full support of current and emerging security standards, including RADIUS, NT Domain Authentication, RSA SecurID, and digital certificates, allows for integration of external authentication systems and interoperability with third-party products
- Advanced packet-filtering capabilities, which provide the required security for your corporate local-area network (LAN)
- User and group-level management for maximum flexibility

High Availability

- Redundant subsystems and multi-chassis fail-over capabilities for maximum system uptime
- Extensive instrumentation and monitoring capabilities, which provide network managers with real-time system status and early-warning alerts

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, Secure Telnet, SSH, and via a console port
- Configuration and monitoring capability for both the enterprise and the service provider
- Access levels are configured by user and groups, allowing easy configuration and maintenance of security policies

Cisco VPN Client (IPsec)

- Available for Windows 95, 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc-32bit), and MAC OS X 10.1.
- Centrally configurable policy management, such as split tunneling/local LAN access policy, is pushed down from the Cisco VPN 3000 Concentrator.

Availability and Ordering Information

Pricing and ordering information can be located at http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm/

A wide variety of service plans are available to support the Cisco VPN 3000 Series Concentrator. Some of these programs include:

Annual Support Plans

Extended Warranty, Enhanced Warranty, 7x24 Installation Support, Remote Telephone Support, Rapid Exchange, Software Subscription

Installation Services

Onsite Installation Service

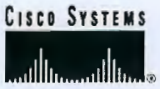
Time and Materials

Repair and Return, Remote Telephone Support (7x24 or M-F/8 -5), Unit Replacement, Software Update, Hardware Configuration

Copyright © 2001 Cisco Systems, Inc. All Rights Reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 158
3698
Doc.

8500
A.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. PIX and SMARTnet are trademarks, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)

0205/DF/DIPE/CN
CPML - CORREIOS
0401/DA
Fls. Nº 159
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1600
Doc. 3698

Cisco Systems

8u99
A.

Data Sheet

CiscoWorks **VPN Monitor** 1.2

Enterprises have recognized the dramatic benefits of virtual private networks (VPNs) using IP Security (IPSec) to reduce costs and secure their networks. Now, as IPSec VPNs become business critical, enterprises need strong management tools to monitor the health of IPSec tunnels and central-site VPN devices.

Introduction

Once a VPN has been deployed, network administrators must be able to monitor the health of the tunnels and VPN devices to ensure optimal VPN services. They need the following information:

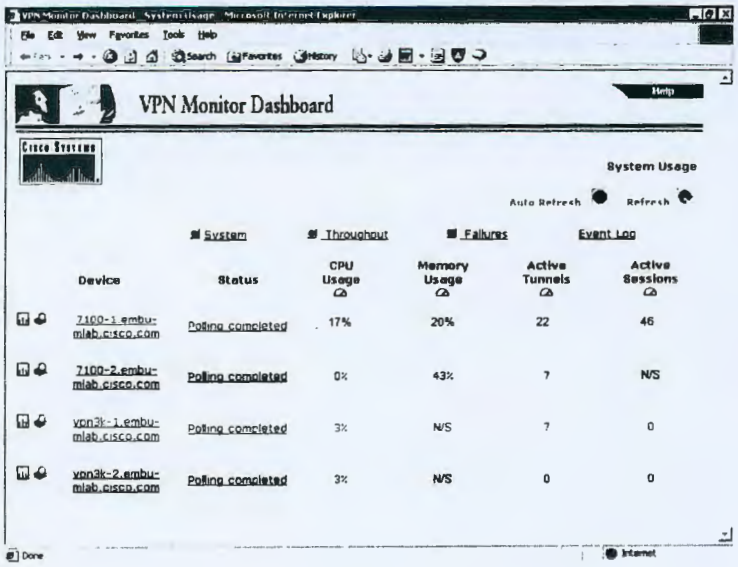
- Number of operational tunnels
- Throughput of individual tunnels
- Status of security negotiations and sessions
- VPN device performance status
- Performance threshold violations

Network managers can generate special reports on VPN-related problems to provide visibility on Internet Key Exchange (IKE), encryption, encapsulation, and certificate problems. Network managers need ongoing reports on current VPN activity, outages, VPN failures, signs of impending failures, and activity history.

CiscoWorks VPN Monitor is a Web-based management tool that allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. CiscoWorks VPN Monitor manages VPNs that are configured on Cisco VPN 3000 concentrators, and Cisco 1700, 2600, 3600, 7100, 7200, or 7400 Series routers. Multiple devices can be viewed from an easy-to-use dashboard configured on a Web browser. After the dashboard is configured, CiscoWorks VPN Monitor continuously collects data from the devices it manages over a rolling seven-day window. Operational status, performance, and security information can be viewed at a glance, providing status information on IPSec VPN implementations.

The dashboard allows network administrators to drill down to further analyze each device's performance and its current IPSec connections. Administrators

Figure 1
CiscoWorks VPN Monitor Dashboard



Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 161
Doc. 3698

8498
A.

can use this drill-down capability to view device CPU and memory performance, tunnel throughput, failure events, threshold violations, and active tunnels on a device. Data collected from VPN devices can also be viewed in detailed graphs that display important parameters related to VPN operation.

CiscoWorks VPN Monitor supports the commonly deployed VPN tunneling protocols, including the IETF Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and IPSec.

Features and Benefits

Flexible Monitoring

CiscoWorks VPN Monitor's configuration flexibility allows network administrators to set polling and graphing intervals to best reflect the network performance of the network and the graphical user interface of CiscoWorks VPN Monitor. The types of monitoring range from the percent utilization of a CPU, to the throughput of a VPN concentrator or router, to the number of users with established connections. Other variables that can be tracked include:

- System resources—average and maximum memory available and CPU utilization percentage per device
- Traffic throughput—average and maximum of encrypted traffic
- Statistics—number of sites that are online, number of sessions established, number of IKE and session failures, and number of current security errors

The dashboard can also provide troubleshooting information. Auto-refreshing Web-based status reports provide detailed information on conditions such as the number of session failures or IKE failures by peer. You can set warnings and alerts based on user-defined threshold values.

Multidevice Comparison

CiscoWorks VPN Monitor provides a convenient way to view important statistics of multiple VPN termination devices in a single dashboard. This capability enables administrators to quickly correct for devices with the highest CPU or memory usage. The multidevice view gives the administrator an aggregated summary of active VPN tunnels and sessions.

Supported Cisco Devices

- Cisco VPN 3000 concentrators with the 2.5.2f software image or later
- Cisco 7100, 7200, or 7400 Series routers with Cisco IOS® Software Release 12.1.(5a)E or later
- Cisco 1700, 2600, and 3600 Series routers with Cisco IOS Software Release 12.2(4)T or later

System Requirements

For comprehensive hardware and operating requirements, see the CiscoWorks VMS Overview at http://www.cisco.com/go/vms

Ordering Information

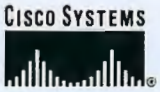
CiscoWorks VPN Monitor is available exclusively as part of the CiscoWorks VPN/Security Management Solution (VMS).

Detailed ordering information is available in the VMS product bulletin at http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 162
Doc. 3698

8497
A.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 163
3698
Doc

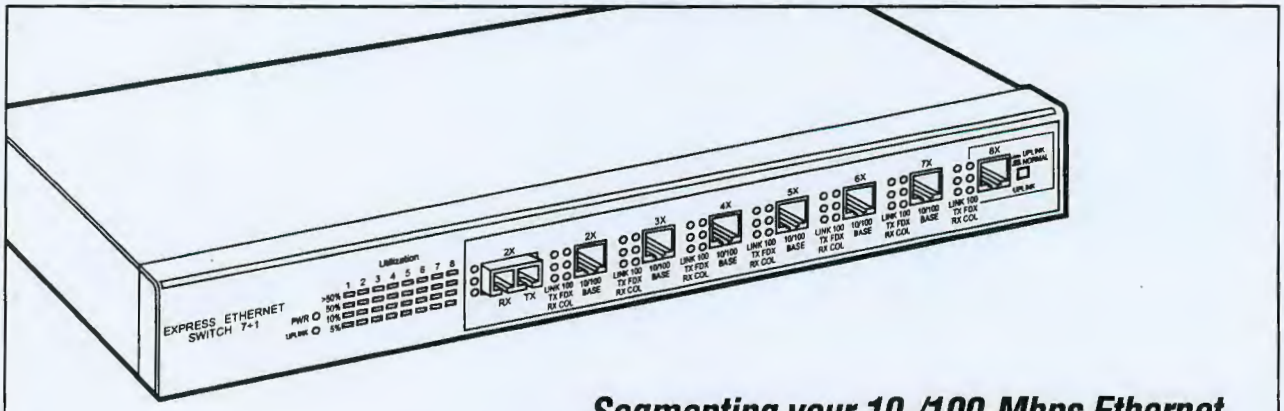
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 164
Doc. 3698

BLACK BOX® NETWORK SERVICES

© 2003. All rights reserved.
Black Box Corporation.

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

EXPRESS ETHERNET SWITCHES



Segmenting your 10-/100-Mbps Ethernet LAN doesn't have to be expensive!

Key Features

- ***Low-cost switching for small- or mid-sized networks.***
- ***Protocol-independent, MAC-layer switching.***
- ***Models for copper, fiber, copper and fiber, or copper with a fiber uplink.***
- ***Fiber ports provide extra distance of over a mile.***
- ***Half-/full-duplex on all RJ-45 ports.***
- ***Reduce bottlenecks.***
- ***Include universal power supply.***

High-speed switching technology at an affordable cost—get the best of both worlds with BLACK BOX® Express Ethernet Switches.

These well-engineered machines provide you with dedicated high-speed workgroups, plus they improve network performance and keep data moving freely and quickly.

Express Ethernet Switches enable you to put a full wire-speed switch right into a network without making a large investment. Plus they're available in a wide variety of port options, from a 2-port model for small network extension to a 24-port switch with optional fiber uplink for mid-sized networks.

And if you want options, these switches have them! Each switch provides true Layer 2 nonblocking switch architecture and a store-and-forward switching engine. With Layer 2 switching, you get the speed to handle lots of network data. The store-and-forward engine checks the integrity of each data packet and ensures accurate throughput.

All Express Ethernet Switches have an autosensing power supply that adapts to worldwide voltages, so they integrate quickly and easily with your existing equipment. A crossover switch makes uplinking to other switches or hubs easy. Extensive LEDs provide port status.

All RJ-45 ports operate at 10/100 Mbps in half- or full-duplex mode. The fiber ports are for 100-Mbps connections in either half-or full-duplex mode.

10-/100-Mbps Copper (LB9108A, LB9019A–LB9020A)

These switches feature 8, 16, or 24 autosensing 10-/100-Mbps RJ-45 ports. They're perfect for rapid, inexpensive network expansion or building workgroups. Because the autosensing ports adjust to the speed and duplexity of each port automatically, setup is a breeze.

The 8-port model supports 1024 MAC address entries and is great for building small workgroups. It's housed in a compact, sturdy enclosure suitable for desktop use or wallmounting.

For higher traffic loads and larger networks, the 16- and 24-port switches support 2048 MAC addresses. A crossover button enables you to configure one port as an uplink. The 16- and 24-port switches include a rackmount kit.

10-/100-Mbps Copper, 100-Mbps Fiber (LB9002A-SC-R2, LB9002A-ST-R2, LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2)

Available in sporty 2-port models or in more robust 8-port versions, these switches divide

1/3/2003 #23276

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 165
Doc. 3698

a network into 10-/100-Mbps copper segments and 100-Mbps fiber segments.

Choose from ST® or SC connectors on the 100BASE-FX side. Each switch has a push-button uplink for linking to another device. Use these switches at the desktop or in racks. Rackmount hardware is included.

The 2-port switches are ideal for adding a 100-Mbps fiber island to your existing network or for extending a network long distances over fiber optic cable. To handle the heavy traffic load associated with this sort of network link, the 2-port switches support a whopping 8192 MAC address entries!

The 8-port switches are good switches for integrating 100-Mbps fiber into your existing 10-/100-Mbps network. The extra distance from fiber means you can extend network segments up to 1.2 miles (2 km).

The LB9006A-SC, LB9006A-ST, LB9021A, and LB9022A models provide DIP switches for controlling port operation manually.

For greater versatility, the LB9007A-R2 models have a console port that enables you to control ports and set up port-based VLANs and trunking. The 8-port switches support 1024 MAC address entries.

Both LB9007A-R2 models support managment. The managament type is an ASCII console port (cable included) that provides access to a text-based menu. The menu permits basic configuration of port parameters (such as changing speed or duplex settings), and has a proprietary method for assigning the ports into VLAN and Port-Trunking groups.

100-Mbps Fiber (LB9008A-FO)

For simplicity, speed, and distance, choose this fiber-only switch. It provides eight ports of blazing speed and distances of up to 1.2 miles (2 km) with all the security of fiber. Best of all, this entry-level switch is super simple to set up—just plug-and-play.

The switch has SC-style fiber connectors and supports 1024 MAC address entries. It has DIP switches and is easy to rackmount with the included hardware.

10-/100-Mbps Copper, 100-Mbps Fiber, Modular (LB9017A-R2, LB9024A) and Optional Fiber Uplink Modules (LB9017C-SC, LB9017C-ST)

These Express Ethernet Switches feature 16 or 24 autosensing 10-/100-Mbps RJ-45 ports. They're a smart-priced way to quickly expand your 10BASE-T/100BASE-TX network with the option of adding a fiber uplink later if you need it.

Although the switches are easy to set up, they offer powerful features to help you control heavy network loads. The 2048 MAC address table handles a large number of end users.

These modular switches also include an RS-232 console port for basic management (cable included). Through the console port, you can access proprietary port-based VLAN features that enable you to segment or isolate traffic at Layer 2.

Trunking provides extra bandwidth of up to 400 Mbps between two connected switches. You can also regulate standard backpressure and auto-negotiation on individual ports. The crossover button enables you to configure one port as an uplink. These switches occupy only 1U of rack space and are easily rackmountable with the included hardware.

Both LB917A-R2 and LB9024A support managment. The managament type is an ASCII console port (cable included) that provides access to a text-based menu. The menu permits basic configuration of port parameters (such as changing speed or duplex settings), and has a proprietary method for assigning the ports into VLAN and Port-Trunking groups.

Specifications

Distance (Maximum):
RJ-45 ports: 100 m (328 ft.);
Fiber ports: 2 km (1.2 mi.)

Forwarding Rate:
14,880 pps at 10 Mbps;
148,800 pps at 100 Mbps

MAC Addresses: LB9108A, LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2, LB9008A-FO: 1024;
LB9002A-SC-R2, LB9002A-ST-R2: 8192;
LB9019A–LB9020A, LB9017A-R2, LB9024A: 2048

Standards: IEEE 802.3 (10BASE-T), IEEE 802.3u (100BASE-TX/FX)

Switching Method: Store-and-forward

VLAN Support: LB9007A-SC-R2, LB9007A-ST-R2, LB9017A-R2, LB9024A: Proprietary port-based

Indicators:
LB9108A:
Per-unit LEDs: (1) Power;
Per-port LEDs:
(1) 100 Mbps/TX,
(1) 10 Mbps/RX,
(1) Full-Duplex/Collision;
LB9019A–LB9020A:
Per-unit LEDs: (1) Power;
Per-TX port LEDs:
(1) Link/Activity, (1) 10-/100-Mbps Speed, (1) Duplex/Collision, (1) 100 Mbps/TX, (1) 10 Mbps/RX, (1) Full-Duplex/Collision;
LB9002A-SC-R2, LB9002A-ST-R2:
Per-unit LEDs: (1) Power;
Per-port LEDs:
(1) Link, (1) 100 Mbps, (1) TX/RX, (1) Duplex/Collision, (4) Utilization;
LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2:
Per-unit LEDs: (1) Power, (1) Uplink;
Per-TX port LEDs:
(1) 10-/100-Mbps Speed, (1) Link, (1) TX, (1) Collision, (1) RX, (1) Duplex, (4) Utilization;
Per-FX port LEDs: (1) Link, (1) Activity, (1) Full-Duplex;
LB9017A-R2, LB9024A:
Per-unit LEDs: (1) Power, (1) Uplink, (1) Module Enable;
Per-TX port LEDs:
(1) 100 Mbps/TX, (1) 10 Mbps/RX, (1) Full-Duplex/Collision;
LB9008A-FO:
Per-unit LEDs: (1) Power, (1) Uplink;
Per-FX port LEDs: (1) Link, (1) Activity, (1) Full-Duplex

Temperature:
Operating: 32 to 104°F (0 to 40°C);
Storage: -13 to +158°F (-25 to +70°C)

Humidity: 10 to 90% noncondensing

Power: 100–240 VAC, 50–60 Hz, autosensing, internal

Size:
LB9108A, LB9002A-SC-R2, LB9002A-ST-R2: 1.4"H x 10"W x 5.3"D (3.6 x 25.4 x 13.5 cm);
LB9019A, LB9021A–LB9022A: 1.75"H x 10.2"W x 8"D (4.4 x 25.9 x 20.3 cm);
LB9020A, LB9006A-SC, LB9006-ST, LB9007A-SC-R2, LB9007A-ST-R2, LB9017A-R2, LB9024A, LB9008A-FO: 1.75"H x 17.3"W x 8"D (4.4 x 43.9 x 20.3 cm)

Weight: LB9108A: 3.5 lb. (1.6 kg);
LB9019A–LB9020A, LB9017A-R2, LB9024A: 5.7 lb. (2.6 kg);
LB9002A-SC-R2, LB9002A-ST-R2: 2.1 lb. (1 kg);
LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2: 5.5 lb. (2.5 kg);
LB9008A-FO: 6.5 lb. (2.9 kg)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 166
3698
Doc.

Layer 2 switching

A switch helps provide a clear path from each workstation to its destination on demand, whether that destination is another workstation or a server. In contrast with bridges and routers (which process data packets on an individual, first-come, first-served basis), switches maintain multiple, simultaneous data conversions among attached LAN segments.

From an end-user workstation's perspective, a switched circuit appears as a dedicated connection—a direct, full-speed LAN link to an attached server or other remote LAN node. Although this technique is somewhat different from what a LAN bridge or router does, switching hubs are based on similar technologies.

Switching hubs that use bridging technologies are called Layer 2 switches—a reference to Layer 2 or the Data Link Layer of the OSI Model. These switches operate using the MAC addresses in Layer 2 and are transparent to network protocols. Layer 2 switches connect different parts of the same network, as determined by the network number contained with the data packet.

If you're subdividing an existing LAN, obviously you're dealing with only one network and one network number, so you can install a Layer 2 switch wherever it will segment network traffic the best, and you don't have to reconfigure the LAN.

If, on the other hand, you use a Layer 3 switch, which uses network addresses, you'd have to reconfigure the segments to ensure that each has a different network number.

Similarly, if you're connecting existing networks, you have to examine the currently configured network numbers before adding a switch. If the network numbers are the same, you need to use a Layer 2 switch. If they're different, you must use a Layer 3 switch.

When dealing with multiple existing networks, you'll find they usually use different network numbers. In this case, it's preferable to use a Layer 3 switch (or possibly even a full-featured router) to avoid reconfiguring the network.

Layer 2 switches are generally unmanaged and are recommended for smaller, less-complex networks.

Store-and-forward switches

Store-and-forward networking switches read each complete data packet into an internal buffer, temporarily storing the packet. The destination and source addresses are checked against the switch's internal address list—just like a bridge. Simultaneously, the entire packet undergoes an error-checking procedure to validate its integrity. This process requires that the whole packet be read, since the check digit is the very last character in the packet. Once verified, the packet is forwarded from the buffer to the appropriate destination device.

Black Box offers the best warranty program in the industry—Fido Protection®. For more information, request **FaxBack 22512**.

Ordering Information

ITEM	CODE
Express Ethernet Switches	
10-/100-Mbps Copper	
(8) RJ-45	LB9108A
(16) RJ-45	LB9019A
(24) RJ-45	LB9020A
10-/100-Mbps Copper, 100-Mbps Fiber	
(1) RJ-45, (1) SC	LB9002A-SC-R2
(1) RJ-45, (1) ST	LB9002A-ST-R2
(2) RJ-45, (6) SC	LB9006A-SC
(2) RJ-45, (6) ST	LB9006A-ST
(6) RJ-45, (2) SC	LB9021A
(6) RJ-45, (2) ST	LB9022A
(7) RJ-45, (1) SC	LB9007A-SC-R2
(7) RJ-45, (1) ST	LB9007A-ST-R2
100-Mbps Fiber	
(8) SC	LB9008A-FO
10-/100-Mbps Copper, 100-Mbps Fiber, Modular	
(16) RJ-45, (1) Slot for Optional Fiber Uplink	LB9017A-R2
(24) RJ-45, (1) Slot for Optional Fiber Uplink	LB9024A
Choose an uplink module for LB9017A-R2 and LB9024A	
100BASE-FX SC Module	LB9017C-SC
100BASE-FX ST Module	LB9007C-ST

NOTE: *The LB9006A–LB9007A models, LB9008A-FO, LB9017A-R2, LB9019A–LB9022A, and LB9024A ship with rack ears.*

For optimum performance and a 20% savings, order...

Category 5 Patch Cable, 100-MHz, 4-Pair, Straight-Pinned, PVC, Beige	EVMSL05
Duplex Fiber Optic Cable, PVC	
ST-ST	EFN062
SC-SC	EFN4025

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 167
3698
Doc.

Apenace III

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1168
Doc. 3698

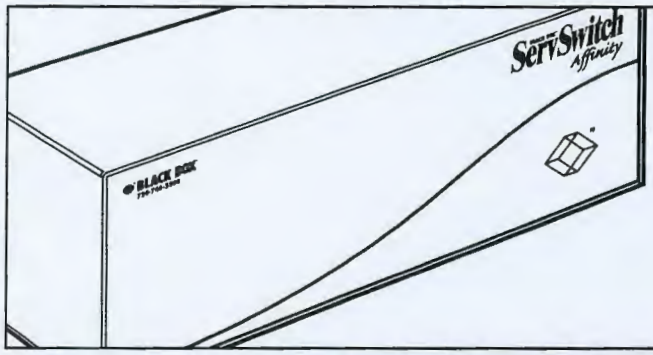
3493
A·

BLACK BOX®
NETWORK SERVICES

© 2001. All rights reserved.
Black Box Corporation.

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

SERVSWITCH™ AFFINITY



Affordable many-to-many multiplatform KVM switching.

Key Features

- ***As many as 16 users have keyboard/mouse/video control over as many as 1024 PC, Sun, RS/6000, SGI, HP, and/or Alpha computers.***
- ***With additional converters, also supports Apple computers.***
- ***Easily expandable with plug-in Port Cards and flexible cabling.***
- ***Free lifetime firmware upgrades.***
- ***Supports video resolutions up to 1280 x 1024.***
- ***High levels of security, including passwords and access profiles.***
- ***Controlled through on-screen display, with additional keyboard commands and a terminal-based serial-port options menu.***
- ***Some models have redundant power supplies.***

Is your server room growing by leaps and bounds? Wouldn't it be nice to have a keyboard/video/mouse-switching system that could keep up with all the hardware, all the users, the constant changes, and the realities of your budget?

Our ServSwitch™ Affinity could be the one. It will support most major hardware platforms, including IBM® PS/2®, PC/AT®, and RS/6000®; Sun®; SGI™; HP® 700 and 9000 series; and Compaq® Alpha™. IBM type computers can use any keyboard mode and any of a variety of mouse types. Video can be any of several types at up to 1280 x 1024 resolution. With additional adapters, you can attach Apple® Macintosh® CPUs too—see **"What else you might need"** on page 4.

You can attach as many as 16 computers to a single unit or 1024 computers to a daisychained Affinity system. Either way, you can also attach up to 4, 8, or 16 independent users; more users can be connected, but they'll have to contend for access.

Here's how it works: Each ServSwitch Affinity has four slots for Port Cards. 0 x 4 Port Cards (product code KV1300C) have four CPU (computer) ports and a serial port only; 1 x 4 Cards (KV1301C) also have a KVM (user) port.

The Affinity chassis also has a fifth, top slot used for expansion purposes; the 16-User models have a matching sixth, bottom slot. 4-User models ship with a Terminator Card (KV1304C) installed in the expansion slot; you can swap in a 4-User Expansion Card (KV1305C) if you'll be daisychaining the Affinity. 8- and 16-User models, which are designed to be part of a daisychain, come without anything installed in the expansion slot(s). You need to purchase and install an 8-User Expansion Card (KV1306C) for each slot in order for the unit to work.

The only difference between the three 4-User Affinity models with single power supplies is which Cards they're preinstalled with; see the start of **"Ordering Information"** on page 5 for a list of which Cards come with each model.

You can add capacity to your Affinity system at any time by installing Port Cards in vacant slots or adding more chassis to a daisychain.

The Port Card's serial ports are used for terminal-based initial system configuration; they are also used to upgrade the Affinity's firmware (upgrades are free for the lifetime of the Affinity!).

The ServSwitch Affinity's main controls are its on-screen menus (with a full range of configuration and operating functions). These menus are augmented by a number of keyboard commands.

For added security, the Affinity supports password-protected access groups. Computers can belong to multiple groups, but users can only belong to one. Users will only be able to access the computers in their group.

When users do access computers, they'll have one of four assigned access levels: view only (no keyboard/mouse control), share (view access until current user becomes inactive, then add keyboard and mouse), control (sole control but others can view), or private (sole control, no one else can interrupt or view).

For mission-critical applications, we offer models of the Affinity with dual, redundant power supplies. If one power supply ever fails, the other can take on the entire load until a replacement supply can be installed.

6/26/2001 #22921

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 169
Doc. 3698

8492
A.

Specifications

Hardware Required: Monitor that supports your computers' highest video standard; in multiplatform applications, should be multisync model that can video from either composite sync or separate horizontal/vertical sync signals

Compliance: CE, FCC Part 15 Subpart J Class A, IC Class/ classe A

Standards:
- With original Serv cabling VGA (color or monochrome/page white) video;
- With original Serv cabling (minimal) or coaxial cabling (recommended): SVGA and (with KV99MA adapter) Mac video;
- With coaxial cabling: XGA (color or monochrome), Sun, RS/6000, or SGI video

Interfaces:
- On CPU ports and user ports of Port Cards and IN 1 and OUT 1 ports of primary Expansion Cards:
  - Proprietary composite of IBM PS/2, PC/AT, or Sun compatible keyboard, PS/2, RS-232 serial (except on user ports), or Sun compatible mouse; and Video (see **Standards** above);
  - With the KV99MCON converter, also supports ADB (Mac compatible) keyboard and mouse ports;
  - IN 1 and OUT 1 also carry system-control signals;
- On Expansion Cards' other IN and OUT ports: Proprietary video composite (see **Standards** above);
- On serial ports of Port Cards: EIA/TIA RS-232 proprietarily pinned on RJ-12 ("6-wire RJ-11") connectors, DTE

Resolution: Up to 1280 x 1024, but will depend on the length of CPU and User Cables in your system

Serial (RS-232) Characteristics:
- Protocol: Asynchronous;
- Data format: 8 data bits, 1 stop bit, no parity (fixed);
- Data rate: 9600 or 57,600 bps

Maximum Distance:
- 20 ft. (6.1 m) of CPU or User Cable—possibly as much as 100 ft. (30.5 m) if Cable is coaxial, depending on CPUs, monitor, and video resolution—from any Affinity Port Card to any device attached to it;
- 100 ft. (30.5 m) of Expansion Cable between any two Affinity units;
- 50 ft. (15.2 m) of serial cable from the RS-232 port of any Affinity Port Card to a computer's serial port

User Controls:
- For system: Keyboard commands and on-screen menus;
- On Affinity chassis: Rear-mounted ON/OFF rocker switch(es); KV13xDA models: (2); All other models: (1);
- On all Expansion Cards (KV1305C and KV1306C): Board-mounted BUS/RING jumper;
- On 8-User Expansion Cards (KV1306C): (2) Board-mounted jumper blocks for user-port numbering

Indicators:
- All models: ON/OFF switch(es) are dark when ServSwitch Affinity is OFF, backlit when Affinity is ON;
- KV13xDA models: (3) Front-mounted power-supply status LEDs:
  - (1) for supply 1 (the upper transformer), lit while supply is outputting power;
  - (1) for supply 2 (the lower transformer), lit while supply is outputting power;
  - (1) for the Affinity chassis (marked "SYSTEM"), lit while either supply is outputting power unless internal diodes have failed

Connectors:
- All rear-mounted;
- On Affinity chassis: IEC 320 male power inlet(s): KV13xDA models: (2); All other models: (1);
- On all Affinity Port Cards (KV1300C and KV1301C):
  - (4) DB25 female for CPU connections,
  - (1) RJ-12 ("6-wire RJ-11") female for serial management;
- On 1 x 4 Port Cards (KV1301C):
  - (1) DB25 female for user connections;
- On 4-User Expansion Cards (KV1305C):
  - (2) DB15 female: (1) for input to Port Cards in slots 1 and 2, (1) for input to Port Cards in slots 3 and 4;
  - (2) DB15 male: (1) for output from Port Cards in slots 1 and 2, (1) for output from Port Cards in slots 3 and 4
- On 8-User Expansion Cards (KV1306C):
  - (4) HD15 female:
    - (1) for input to Port Cards set as KVM 1/2 or 9/10;
    - (1) for input to Port Cards set as KVM 3/4 or 11/12;
    - (1) for input to Port Cards set as KVM 5/6 or 13/14;
    - (1) for input to Port Cards set as KVM 7/8 or 15/16;
  - (4) HD15 male:
    - (1) for output from Port Cards set as KVM 1/2 or 9/10;
    - (1) for output from Port Cards set as KVM 3/4 or 11/12;
    - (1) for output from Port Cards set as KVM 5/6 or 13/14;
    - (1) for output from Port Cards set as KVM 7/8 or 15/16

Maximum Altitude:
10,000 ft. (3048 m)

Temperature Tolerance:
32 to 113°F (0 to 45°C)

Humidity Tolerance:
5 to 80% noncondensing

Enclosure: Steel

Fuses: KV13xDA models: Autoresetting switch fuses that cut in when power surges exceed the maximum ratings of the chassis

Power:
- Input: 90 to 264 VAC, 47 to 63 Hz, 700 mA from AC outlet(s) through included power cord(s) and inlet(s) into internal transformer(s): KV13xDA models: Dual transformers with separate AC inlets, electrically isolated from one another; All other models: Single transformer;
- Consumption: Up to 40 VA (40 watts)

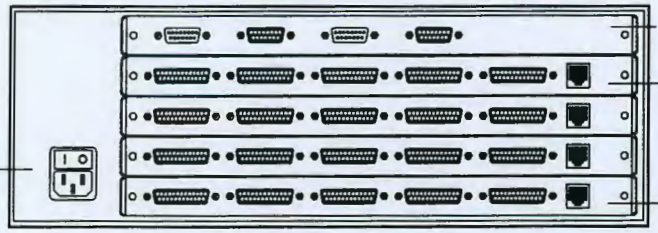
Size:
- KV139A and KV139DA chassis: 7"H (4U) x 16.7"W x 7"D (17.8 x 42.4 x 17.8 cm);
- All other Affinity chassis: 5.25"H (3U) x 16.7"W x 7"D (13.3 x 42.4 x 17.8 cm);
- Port Cards and Expansion Cards: 0.9"H x 13.9"W x 4.8"D (2.3 x 35.3 x 12.2 cm);
- Terminator Card (4-User models only): 0.4"H x 2.1"W x 0.8"D (1 x 5.3 x 2 cm)

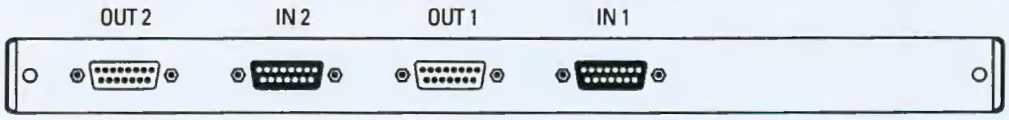
Weight:
- KV130A, KV130DA, KV138A, and KV138DA: 10.5 lb. (4.8 kg);
- KV132A: 12 lb. (5.5 kg);
- KV134A: 14 lb. (6.4 kg);
- KV139A and KV139DA: 11 lb. (5 kg);
- KV1300C, KV1301C, and KV1306C: 0.9 lb. (0.4 kg);
- KV1304C: 0.2 lb. (0.1 kg);
- KV1305C: 0.4 lb. (0.2 kg)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 170
Doc. 3698

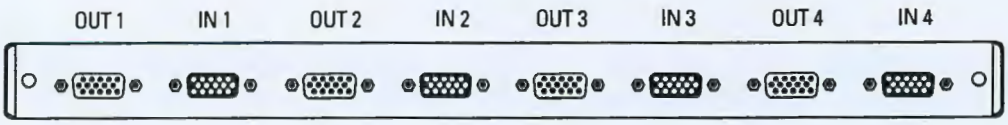
If you need to share access to a large number of CPUs, think about putting in an Affinity daisychain made up of 4-User Expansion Chassis (like the fully loaded one shown below) or 8- or 16-User Chassis. They come empty (no Cards installed), but you can install one Expansion Card (or two in the 16-User units) and add as many as four 0 x 4 or 1 x 4 Port Cards to them, giving you a maximum of four, eight, or sixteen user stations and sixteen CPUs attached to each unit. (Keep in mind that however many user stations a unit is designed for, only that many video paths can be open through that unit at a time. For example, a 4-User unit only has four video paths, so if there are already four users attached to a 4-User unit, and a user at another Affinity unit selects one of the 4-User unit's CPUs, one of the 4-User unit's users—and all other users on that slot—will be locked out until the new connection ends.)

The 8-User units look very similar to the 4-User unit shown here, but they accept only 8-User Expansion Cards like the one shown below. The 16-User units accept two of the 8-User Expansion Cards. The 8-User Cards have jumper blocks that you can set to control which four KVM slots are used by the users attached to the Affinity chassis that the Card is installed in: KVM 1 through 4, 5 through 8, 9 through 12, or 13 through 16.





DB15 female expansion ports on 4-User Expansion Card (KV1305C)



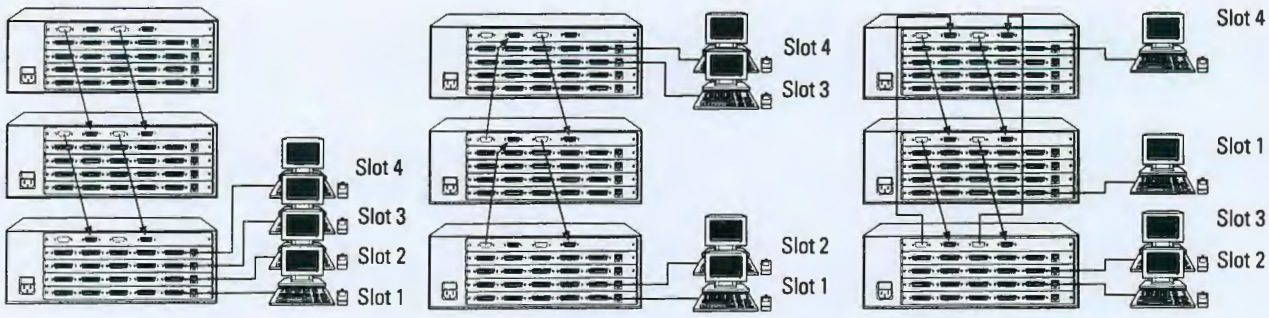
HD15 female expansion ports on 8- and 16-User Expansion Card (KV1306C)

On the 4-User Expansion Cards (above, top), IN 1 and OUT 1 carry signals for the Port Cards in slots 1 and 2, while IN 2 and OUT 2 carry signals for the Port Cards in slots 3 and 4.

On the 8-User Expansion Cards (above, bottom), IN 1 and OUT 1 carry the signals for either KVM 1 and 2 or, if installed in the bottom slot of a 16-User unit, KVM 9 and 10; IN 2 and OUT 2 cary the signals for either KVM 3 and 4 or KVM 11 and 12; and so on. A pair of jumper blocks, mentioned above, determines which four KVM slots the four users on that Affinity chassis will use.

Because the control paths are carried on different connectors this way, you have maximum flexibility for designing your daisychain layout:

- If all of your users are on one Chassis, use the regular bus topology (below, left).
- If you have two users on one Chassis and two on another, use the "split bus" topology (below, middle).
- If your users are spread across several Chassis, use the ring topology (below, right).*



Regular Bus Split Bus Ring

*It is always important to keep in mind that only one user at a time can use the bus that interconnects daisychained Affinity units, especially when you implement a ring topology. For example, when your Affinity units are interconnected in a ring, if any user on Slot 1 selects a CPU attached to an Affinity unit other than his own, no other Slot 1 user can select any CPUs.

ECTQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 171
Doc. 3698

8490
A.

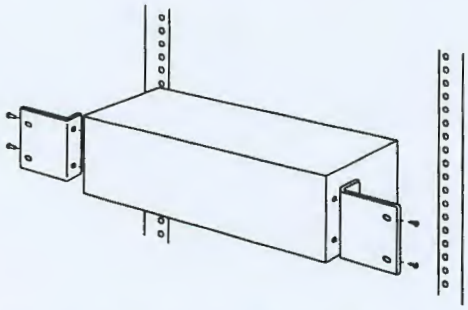
The complete package

- The ServSwitch Affinity, including any cards and blanking plates that are normally preinstalled with your model. (Blanking plates will cover all unused slots, as well as the slot on 4-User models that the tiny Terminator Card is installed in.)
- A power cord.
- *KV13xDA models only:* A second power cord.
- A 6-ft. (1.8-m) serial cable with RJ-12 ("6-wire RJ-11") plugs.
- An RJ-12 to DB9 modular adapter.
- A manual.

What else you might need

- CPU Adapter Cables, User Adapter Cables, and (if you're cascading) Expansion Cables.
- Keyboards, mice, and monitors for your users. If you're mixing platforms, we recommend true multiscan, multisync monitors capable of syncing to each CPU's video-output frequencies and compatible with all of the CPUs' video cards. Also, if one of the multiple platforms is IBM, the monitors must be able to accept both separate H/V sync and composite sync. (Such monitors are widely available.) We recommend that the monitors be able to display a maximum resolution of not less than 1280 x 1024 at a maximum refresh rate of not less than 75 Hz.
- An AC-power surge protector and uninterruptible power supply.
- Data-line surge protectors for the keyboard and mouse lines.
- *To attach an Apple Mac®:* A ServSwitch™ Micro Mac® Converter (product code KV99MCON), a G3™/G4™ or legacy Macintosh® style CPU-Extension Cable, and, if the Mac needs to see ID bits from its monitor, a Mac Video Adapter for ServSwitch (KV99MA).
- *If you purchase a 4-User Expansion Chassis or an 8- or 16-User Chassis:* Port Cards for your CPU and user-station connections.
- *To cascade a ServSwitch Affinity:* An Expansion Card.
- *To rackmount a ServSwitch Affinity:* A ServSwitch Affinity Rackmount Kit.

If you can use a screwdriver, you can install the Rackmount Kits.



Ordering Information

ITEM	CODE
ServSwitch Affinity	
4-User Expansion Chassis (Terminator Card installed, no Port Cards installed)	
Single power supply	KV130A
Dual power supply	KV130DA
4-User Standalone Chassis:	
2 Users by 8 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 and 2)	KV132A
4 Users by 16 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 through 4)	KV134A
8-User Chassis (no Cards installed)	
Single power supply	KV138A
Dual power supply	KV138DA
16-User Chassis (no Cards installed)	
Single power supply	KV139A
Dual power supply	KV139DA
Port Cards	
0 x 4 (No Users, Four CPUs)	KV1300C
1 x 4 (One User, Four CPUs)	KV1301C
4-User Terminator Card	KV1304C
4-User Expansion Card	KV1305C
8- and 16-User Expansion Card	KV1306C

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 172
Doc. 3698

Ordering Information (continued)

ITEM	CODE

NOTE: For CPU and User Cables, specify length by adding any of these suffixes to the product code (not all cables are available in all lengths):
"-0001" for 1 ft. (0.3 m, User Cables only),
"-0005" for 5 ft. (1.5 m),
"-0010" for 10 ft. (3 m),
"-0020" for 20 ft. (6.1 m),
"-0035" for 35 ft. (10.7 m),
"-0050" for 50 ft. (15.2 m),
"-0075" for 75 ft. (22.8 m), or
"-0100" for 100 ft. (30.5 m)

*You will need a **CPU Cable** for each CPU you attach:*

Standard CPU Cables, available in standard lengths up to 20 ft. (6.1 m)—Mac styles require keyboard/mouse conversion

IBM PS/2 style	EHN051
IBM PC/AT style	EHN048
Mac style with legacy DB15 video connectors	EHN215
Mac style with HD15 VGA video connectors for G3™, G4™, and similar models	EHN550

Coaxial CPU Cables—IBM and Sun styles available in all standard lengths, SGI and RS/6000 styles available in standard lengths up to 20 ft. (6.1 m), Mac styles require keyboard/mouse conversion

Universal IBM style	EHN282
Sun style with traditional 13W3 video connectors	EHN206
Sun style with VGA (HD15) video connectors	EHN515
SGI style	EHN500
RS/6000 style	EHN520
Mac style with traditional DB15 video connectors	EHN208
Mac style with HD15 VGA video connectors for G3, G4, and similar models	EHN560

ServSwitch™ Micro Mac® Converter to convert PS/2 kbd/mouse to ADB™ kbd/mouse signals	KV99MCON
For older Mac models that must see monitor ID: Mac® Video Adapter for ServSwitch™	KV99MA

*You will need a **User Cable** for each monitor/keyboard/mouse user station you attach:*

Regular (non-coaxial) User Cables, available in standard lengths up to 20 ft. (6.1 m)

IBM PS/2* style	EHN054
Sun style with VGA (HD15) video connector for multisync monitor	EHN059

Coaxial User Cables

IBM PS/2* style, available in all standard lengths except 1 ft. (0.3 m)	EHN283
Sun style with 13W3 video connector for Sun monitor, available in all standard lengths	EHN201
Sun style with VGA (HD15) video connector for multisync monitor, available in all standard lengths	EHN225
SGI style, 1 ft. (0.3 m) only	EHN501-0001
RS/6000 style, 1 ft. (0.3 m) only	EHN521-0001

*We no longer offer IBM PC/AT type User Cables for the ServSwitch Affinity, because its current firmware does not support serial mice, although it will still translate signals from PS/2 type mice into serial protocol for PC/AT CPUs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 173
Doc. 3698

8488
A.

Ordering Information (continued)

ITEM	CODE
You might also need:	
Expansion Cables for 4-User Units	
10 ft. (3 m)	KV140010
20 ft. (6.1 m)	KV140020
35 ft. (10.7 m)	KV140035
50 ft. (15.2 m)	KV140050
100 ft. (30.5 m)	KV140100
Expansion Cables for 8- and 16-User Units	
10 ft. (3 m)	KV180010
20 ft. (6.1 m)	KV180020
35 ft. (10.7 m)	KV180035
50 ft. (15.2 m)	KV180050
100 ft. (30.5 m)	KV180100
Replacement 6-wire straight-through-pinned flat-satin cable for serial management (specify length)	EL06MS-MM
Rackmount Kits	
To mount 4- or 8-User units in 19" Racks	RMK19A
To mount 4- or 8-User units in 23" Racks	RMK23A
To mount 4- or 8-User units in 24" Racks	RMK24A
To mount 16-User units in 19" Racks	RMK19A139
To mount 16-User units in 23" Racks	RMK23A139
To mount 16-User units in 24" Racks	RMK24A139
Surge protector for IBM PS/2 style keyboard and mouse lines (6-pin mini-DIN M/F)	SP519A-R2
Surge protector for IBM PC/AT style keyboard lines (5-pin DIN M/F)	SP518A-R2

Call Black Box Tech Support for help determining your best options for AC-power backup and protection.

Black Box offers the best warranty program in the industry—Fido Protection®. For more information, request **FaxBack 22512**.

BLACK BOX, the ◆ logo, and Fido Protection are registered trademarks, and ServSwitch and ServSwitch Affinity are trademarks, of Black Box Corporation.

All other trademarks mentioned in this document are acknowledged to be the property of the trademark owners.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 171
Doc. 3691

Apêndice HF

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 175
Doc. 3698

8487
A.

QuickSpecs

Compaq USB & PS/2 Keyboard and Mouse

MODELS

Compaq USB & PS/2 Keyboard
118003-009

Compaq USB & PS/2 Mouse
103180-B22

OVERVIEW

The Compaq USB & PS/2 Easy Access Keyboard provides all the functionality of a USB, PS/2, and windows keys compatible keyboard, and also offers eight "easy access buttons " The keyboard connects to a standard USB port and also comes equipped with a USB to PS/2 adapter that converts from a USB Series connection to a PS/2 connection.

Easy Access Keyboards facilitate frequent use of the Internet by providing easy, immediate access to Web-based information at the touch of a button. Users who repeatedly access Internet or intranet web sites will appreciate the expanded functionality and ease of use of these keyboards. Through the client-based Easy Access Keyboard software utility, they can customize the eight pre-programmed buttons to gain instant access to Internet addresses, applications, or files

The Compaq USB & PS/2 Mouse is a two-button mouse with scroll wheel that provides the speed and accuracy of optical tracking in a simple, elegant design. It plugs into either a USB or PS/2 port through an adapter and records motion precisely on a variety of surfaces using the latest optical sensing technology. The Compaq USB Mouse has no ball or moving parts, which improves its durability, makes it require less cleaning, and eliminates sticking. The mouse's comfortable, contoured shape fits either hand.

Key Benefits

Keyboard

- Saves time and effort by directing users instantly to targeted Internet destinations
- Allows customized programming of buttons to launch user-specified applications
- Features pre-programmed buttons for easy access to useful business web sites
- Connects to USB or PS/2 ports

Mouse

- Improves precision by using optical tracking
- Provides more durability and easier maintenance by eliminating moving parts
- Fits either hand
- Allows scroll wheel to function as a third button
- Connects to USB or PS/2 ports

COMPATIBILITY

The Compaq USB & PS/2 Keyboard and Mouse are compatible across all HP notebooks.

SERVICE AND SUPPORT

The Compaq USB & PS/2 Keyboard and Mouse have a one-year limited warranty or the remainder of the warranty of the HP product in which it is installed. Technical support is available seven days a week, 24 hours a day by phone, as well as in online support forums. Certain restrictions and exclusions apply

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 176
Doc. 3698

8486 A.

SPECIFICATIONS

Compaq USB & PS/2 Keyboard
118003-009

Physical characteristics	**Keys**	104, 105, 106, 107, 109 layout (depending upon country) plus eight programmable keys for Internet, shortcuts, or multimedia
	Dimensions (L x W x H)	18.0 x 6.3 x 1.3 in (45.8 x 16.1 x 3.3 cm)
	Color	Compaq carbon
	Weight	2 lb (0.9 kg) minimum
Electrical	**Operating voltage**	+5VDC +/- 5%
	Power consumption	50-mA maximum (with three LEDs ON)
	System interface	USB & PS/2 combo
	ESD	CE level 4, 15-kV air discharge
	EMI - RFI	Conforms to FCC rules for a Class B computing device
	Microsoft PC 99 - 2001	Functionally compliant
Mechanical	**Languages**	30+ available
	Keycaps	Low-profile design
	Switch actuation	55-g nominal peak force with tactile feedback
	Switch life	20 million keystrokes (using Hasco® modified tester)
	Switch type	Contamination-resistant membrane
	Key-leveling mechanisms	For all double-wide and greater-length keys
	Cable length	6 ft (1.8 m)
	Microsoft PC 99 - 2001	Mechanically compliant
	Acoustics	43-dBA maximum sound pressure level
Environmental	**Operating temperature**	50° to 122° F (10° to 50° C)
	Non-operating temperature	–22° to 140° F (–30° to 60° C)
	Operating humidity	10% to 90% (non-condensing at ambient)
	Non-operating humidity	20% to 80% (non-condensing at ambient)
	Operating shock	40 g, six surfaces
	Non-operating shock	80 g, six surfaces
	Operating vibration	2-g peak acceleration
	Non-operating vibration	4-g peak acceleration
	Drop (out of box)	26 in (66 cm) on carpet, six-drop sequence
	Drop (in box)	42 in (107 cm) on concrete, 16-drop sequence
Operating system support	Microsoft Windows 2000, and XP	
Approvals	CE-Mark, UL, CSA, FCC Class B, C.I.S.P.R, ACE Class B, ICES-003 class B, VDE/TUV, VCCI, BSMI, MIC	
Ergonomic compliance	ANSI/HFS 100, ISO 9241-4, and GS Mark	
Kit contents	Keyboard, keyboard software media, installation guide, warranty card, safety and comfort guide, USB/PS2 Adapter	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 177
Doc. 3698

8485 A-

SPECIFICATIONS *(continued)*

Compaq USB & PS/2 Optical Wheel Mouse
103180-B22

Physical characteristics	**Dimensions** (L x W x H)	4.6 x 2.5 x 1.5 in (116.4 x 62.5 x 38 mm)
	Weight	0.28 lb (130 g)
Electrical	**Supply voltage** (USB mode)	5.0V
	Supply voltage (PS/2 mode)	5.0V
	Power consumption	95-mA maximum
	System interface	USB & PS/2 combo
	ESD	IEC 801-2 level 4, no damage up to15-kV
Mechanical	**Cable length**	6 ft (1850 mm)
Environmental	**Operating temperature**	–32° to 104° F (0° to 40° C)
	Non-operating temperature	–4° to 140° F (–20° to 60° C)
	Operating humidity	10% to 90% (non-condensing at ambient)
	Drop	32 in (80 cm) on asphalt tile over concrete, five-drop sequence
Operating system support	Microsoft Windows 98, 2000, NT 4.0, ME and XP	
Approvals	CE-Mark, UL, FCC Class B, TUV GS EN 60950, VCCI, BCIQ, C-Tick, RRL, ABNT-2	
Kit contents	Mouse, USB/PS2 adapter, documentation	

HP recommends Microsoft® Windows® XP Professional for Mobile Computing

© 2003 Hewlett-Packard Company

Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided 'as is' without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty. The information in this publication is subject to change without notice.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 178
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 179
Doc. 3698

QuickSpecs

Compaq Evo Notebook N1020v

Overview

What's New

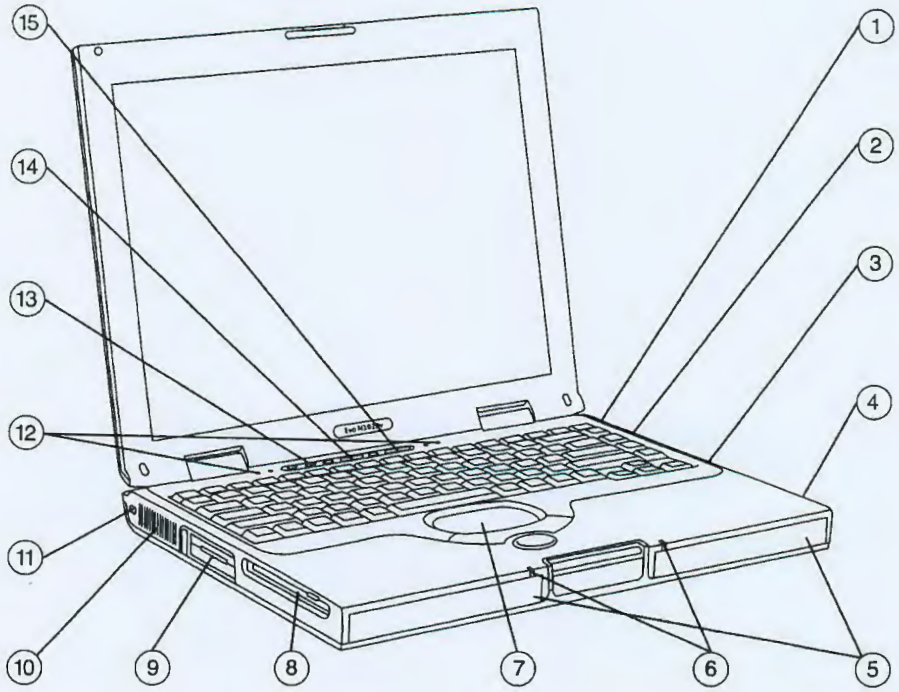
- Intel® Pentium® 4 processors – up to 2.4 GHz; Intel Celeron® processors – up to 1.6 GHz
- 400-MHz bus
- 4X AGP Graphics
- MultiPort wireless communication options
- Touchpad

At A Glance

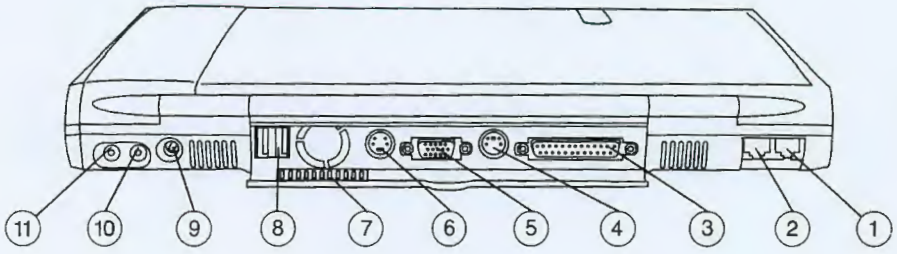
- Intel Pentium 4 processors – up to 2.4 GHz; Intel Celeron processors – up to 1.6 GHz
- 15-inch XGA and 14.1-inch XGA display
- Configurations as light as 6.6 lb (3 kg) weight (14-inch panel)
- 1.55 in (3.95 cm) thin
- 256 MB DDR SDRAM (266 MHz). Upgradeable to 1024 ME
- 20,30 or 40 GB SMART hard drives
- Mini PCI modem and integrated NIC
- Full-size keyboard
- Microsoft® Windows® XP Pro and XP Home
- Includes a one-year, Worldwide Warranty. —Certain restrictions and exclusions apply. Consult the Compaq Customer Support Center for details.

What's Special

- Intel Pentium 4 processors
- All-in-one convenient design
- Latest USB 2.0 interface
- Wireless features thru award-winning MultiPort
- Common Docking Options



1. 1394
2. Infrared
3. Optical Drive
4. Battery
5. Stereo Speakers
6. System LEDs
7. Touchpad
8. Diskette Drive
9. PC Card Slot (1)
10. Kensington Lock
11. Air Vent
12. Keyboard LEDs
13. Easy Access Buttons
14. Power Button
15. Volume Control



1. RJ-11
2. RJ-45
3. Parallel
4. PS/2
5. VGA
6. S-video
7. Air Vent
8. USB
9. DC in
10 Audio in
11. Headphone

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 180
Doc. 3698

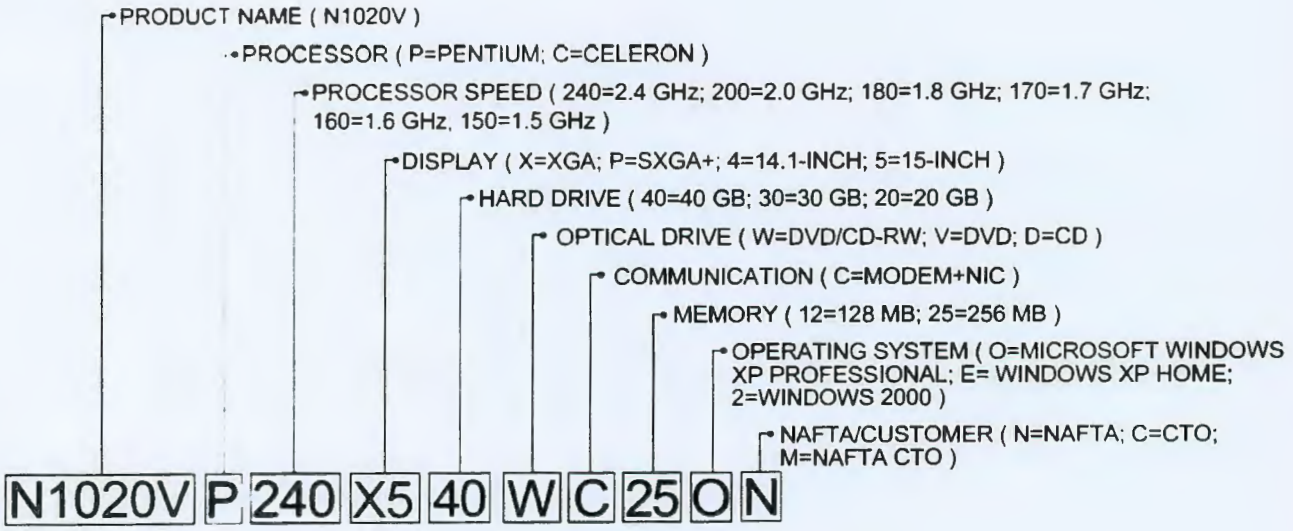
8442 A.

Standard Features

Multimedia	JBL Pro Speakers with bass reflex and 16bit stereo sound Dedicated Hardware volume controls Headphone-out port Microphone in port Software MPEG1 support, MPEG2 and DVD 8X DVD/CD-RW Combination Drive (on select models) 8X DVD-ROM Drive with movie playback software (on select models) 24X CD-ROM Drive (on select models) S-video Port IEEE 1394 Port 4X AGP graphics 32 MB of DDR (Double Date Rate) SDRAM	
Interfaces	PC Card	One Type II
	Enhanced Parallel EPP/ECP	1
	PS/2	1
	S-Video	1
	VGA	1
	1394	1
	Port Replicator	1
	Headphone/Line-out	1
	DC Power	1
	RJ-11 (modem)	1
	RJ-45 (NIC)	1
	Infrared Port	1 (4 Mb/s support) (IrDA 4 MB compliant. IR performance will vary depending on performance of IR peripherals and application used.)
	USB Port	2
	LED status indicators	6
Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator with 32-MB DDR shared video memory for increased color depth and graphics performance	
Display (External)	Up to 32-bit per pixel color depth Supports 640 x 480, 800 x 600, 1024 x 768, 1280 x 1024, 1400 x 1050, 1600 x 1200, or 2048 x 1536 resolutions up to 160-Hz refresh rate, dependent upon monitor capability, resolution and color depth settings	
Display (Internal)	14.1-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal) 15-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal)	
Operating System	Microsoft Windows XP Pro, or Microsoft Windows XP Home preinstalled	
Software	Diagnostics for Microsoft Windows DVD Playback Software Compaq Security Management Safety and Comfort Guide Acrobat Reader Reference Guide Compaq Easy Access Button Software	
System Recovery	Each unit is shipped with a CD kit for quick recovery (erases hard disk and restores manufacturer installed image) and software recovery (installs only selected standard software)	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 181
Doc. 3608

Naming Convention The Etymology of a Model name:



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 182
Doc. 3698

8438

A.

Standard Features

MODELS *(continued)*

N1020vC160X420DC25O	**Display**	14.1-inch color TFT XGA
P/N 470047-364	**Processor**	1.60 GHz Celeron
	Cache Memory	256 KB, L2 Cache
	Standard Memory	256MB (1 DIMM) 266 MHz DDR
	Maximum Memoru	1024 MB (266 MHz) DDR
	Optical Drive	20GB
	Hard Drive	24X CD-ROM Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Pro
	Warranty	One Year

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 183
Doc. 3698

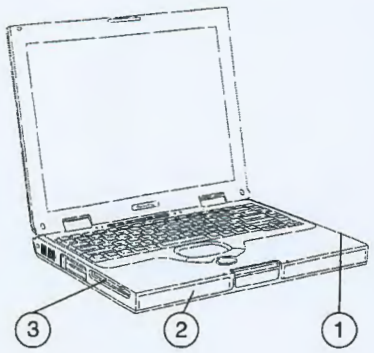
8436
A.

Options

Input Devices	External Enhanced III Keyboard (carbon)	118003-008
	Compaq 2 Button Mouse (carbon)	103180-B21
	USB 2 Button Scroll Mouse (carbon)	195255-B25
	External 10-Key Numeric Keypad (carbon)	294317-B21
	USB EZ Access Keyboard	222726-008
Security	Biometric PC Card	146805-B25
	Security Cable Lock	294316-B21
	Compaq Smart Card PC Card Reader	135646-B25
Useful Accessories	Compaq iPAQ Microportable Projector MP1200	261966-001
	Compaq iPAQ Microportable Projector MP3800	262839-001
	Compaq iPAQ Microportable Projector MP4800	257524-001
	Lamp Module L20 for MP1200	266631-B24
	Lamp Module L30 for MP3800	266633-B24
	Home Theatre Kit HT150 for MP3800	292187-B24
	Carrying Case for MP1200	295731-B24
	Lamp Replacement Kit for MP1600	118052-001
	Lamp Module for MP1800, MP1400	189789-001
	Lamp Module for MP2800, MP2810	215464-001
	Home Theater Kit HT110 for MP1410	246161-001
	Multimedia Adapter & Remote Control Kit MMA110 for MP1410	246162-001
	Multimedia Adapter & Remote Control Kit for MP1400, MP1800	174963-001
	Deluxe Carrying Case for MP Series projectors	253364-001
	Lamp Module for MP1410, MP1810	253365-001
	Lamp Module L90 for MP4800	257892-001
	Home Theater Kit HT180 for MP1200, MP4800	281729-001
	CeilingMount Kit CM10 for MP1200, MP4800	281730-001
	hp digital projector sb21	L1510A
	hp digital projector xb31	L1511A
	Ceiling Mount Kit for xb31	L1513A
	M1-A to component/USB video cable for sb21, xb31	L1523A
	M1-D to DVI/USB cable for sb21, xb31	L1529A
	Lamp Module for sb21	L1515A
	Lamp Module for xb31	L1516A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 184
Doc. 3698

Storage



1. Dedicated optical drive
2. Primary hard drive
3. Dedicated diskette drive

DRIVE SUPPORT

System Drive Support	Quantity Supported	Drive Supported
1.44-MB Diskette Drive	1	Dedicated diskette drive
DVD/CD-RW Combo Drive	1	Dedicated optical drive
DVD-ROM Drive	1	Dedicated optical drive
Max CD-ROM Drive	1	Dedicated optical drive
Hard Drives		
40-GB SMART Hard Drive	1	Dedicated hard drive bay
30-GB SMART Hard Drive	1	Dedicated hard drive bay
20-GB SMART Hard Drive	1	Dedicated hard drive bay

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 189
3698
Doc.

Technical Specifications

14.1-Inch Color TFT XGA Display	**Dimensions** (H x W)	11.22 x 8.46 in (28.5 x 21.5 cm)	
	Diagonal Size	14.1 in (35.81 cm)	
	Mounting	Internal Panel Supports, Side Mounted	
	Number of Colors	Up to 16.8M	
	Contrast Ratio	150:1	
	Brightness	120nt typ	
	Pixel Resolution	Pitch	0.264 x 0.264 mm
		Format	1024 x 768
		Configuration	RGB stripe
	Backlight	Edge Lit	
	Character Display	80 x 25	
	Total Power Consumption	4.2W	
15-Inch Color TFT SXGA+ Display	**Dimensions** (H x W)	11.8 x 9 in (30.4 x 22.8 cm)	
	Diagonal Size	15 in (38 cm)	
	Mounting	Internal Panel Supports, Side Mounted	
	Number of Colors	Up to 16.8M	
	Contrast Ratio	150:1	
	Brightness	150nt typ	
	Pixel Resolution	Pitch	0.218264 x 0.218264 mm
		Format	1400 x 1050
		Configuration	RGB stripe
	Backlight	Edge Lit	
	Character Display	80 x 25	
	Total Power Consumption	5.75W	
15-Inch Color TFT XGA Display	**Dimensions** (H x W)	11.8 x 9 in (30.4 x 22.8 cm)	
	Diagonal Size	15 in (38 cm)	
	Mounting	Internal Panel Supports, Side Mounted	
	Number of Colors	Up to 16.8M	
	Contrast Ratio	150:1	
	Brightness	150nt typ	
	Pixel Resolution	Pitch	0.297 x 0.297 mm
		Format	1024 x 768
		Configuration	RGB stripe
	Backlight	Edge Lit	
	Character Display	80 x 25	
	Total Power Consumption	5.0W	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 186
Doc. 3698

Technical Specifications

Hard Drives *(contiuned)*

30-GB	**Drive Weight**	0.22 lb (99 g)	
	Capacity	30 GB	
	Height	0.374 in (9.5 mm)	
	Width	2.75 in (70 mm)	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	2.5 ms
		Average	12 ms
		Maximum	23 ms
	Rotational Speed	4200 rpm	
	Logical Blocks	58,605,120	
	Operating Temperature	41° to 131° F (5° to 55° C)	
20-GB	**Drive Weight**	0.21 lb (95 g)	
	Capacity	20 GB	
	Height	0.374 in (9.5 mm)	
	Width	2.75 in (70 mm)	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	2.5 ms
		Average	12 ms
		Maximum	23 ms
	Rotational Speed	4200 rpm	
	Logical Blocks	~ 39,070,080	
	Operating Temperature	41° to 131° F (5° to 55° C)	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 187
Doc. 6088

Technical Specifications

DVD/CD-RW Drive	**Center Hole Diameter**	15 mm	
	Disk Diameter	12 cm, 8 cm	
	Disk Thickness	1.2 mm	
	Track Pitch	1.6 µm	
	Access Times (typical reads, including settling)	Random CD	< 120 ms
		Full-Stroke CD	< 175 ms
	Disk Diameter	Random DVD	< 140 ms
	Disk Thickness	Full-Stroke DVD	< 225 ms
	Audio Output Level	0.7 – 0.9 Vrms	
	Cache Buffer	2 Mbytes (minimum)	
	Data Transfer Rate (typical, including settling)	CD-R (8X)	1200 KB/s (150 KB/s at 1X CD rate)
		CD-RW (8X)	1200 KB/s (150 KB/s at 1X CD rate)
		CD-ROM (24X)	3600 KB/s (150 KB/s at 1X CD rate)
		DVD (8X)	10,800 KB/s (1352 KB/s at 1X DVD rate)
		Normal PIO Mode 4 (single burst)	16.6 MB/s
	Start-up Time	Single	< 7 seconds (typical)
		Multi-Session	< 30 seconds (typical)
	Stop Time	< 3 seconds (typical)	
DVD-ROM Drive	**Center Hole Diameter**	0.59 in (1.5 cm)	
	Disc Diameter	12 cm/8 cm	
	Disc Thickness	1.2 mm	
	Track Pitch	0.74 µm	
	Access Times (typical reads, including settling)	Random (typical)	< 125 ms DVD Media
		Full-Stroke (typical)	< 225 ms DVD Media
		Random (typical)	< 100 ms CD Media
		Full-Stroke (typical)	< 175 ms CD Media
	Cache Buffer	512 KB/s (minimum)	
	Data Transfer Rate (typical, including settling)	Max 24X CD	3600 KB/s (150 KB/s at 1X CD rate)
		Max 8X DVD	10,800 KB/s (1352 KB/s at 1X DVD rate)
	Start-up Time	< 12 seconds Typical	
	Stop Time	< 3 seconds Typical	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 188
3698
Doc.

8426 A.

Technical Specifications

802.11b MultiPort Module *(continued)*	**Network Architecture Models**	Ad-hoc (Peer to Peer)
		Infrastructure (Access Points Required)
	Modulation Technique	Direct Sequence Spread Spectrum: DBPSK, DQPSK, CCK
	Receiver Sensitivity – Bit Error Rate (1E-5)	11 Mbps: -85 dBm
		5.5 Mbps: -87 dBm
		2 Mbps: -91 dBm
		1 Mbps: -94 dBm
	Maximum Receive Level	–4 dBm
	Output Power (approximately)	18 dBM
	Operating Voltage	5V power operation
	Power Management	Keystroke Fn+F2 Power On/Off control
	Power Consumption	Transfer mode: < 600 mA, maximum
		Receive mode: > 400 mA, maximum
		Standby mode: > 1 mA, maximum
	Transmit Power	10 to 100mW It is preferable to have the user configurable output power to save battery life for laptop users or in high AP coverage areas
	Power Saving Option	802.11 Compliant Power Saving
		Power Saving Mode selectable through the configuration utility
		ACPI compliant power management
	Media Access Protocol	CSMA/CA (Collision Avoidance) with ACK
	OS Support	Microsoft Windows 2000
		Microsoft Windows XP Home
		Microsoft Windows XP Pro
	Protocols Supported	TCP/IP
		IPX/SPX
		UDP
	LED Activity	Flashing LED – AP Search Mode
		Solid LED – On
		LED Off – Power Off

Throughput, Data Rate and Operating Distance	**Throughput**	**Data Rate**	**Operating Distance**
	> 4.5 Mbps	11 Mbps	• 1000 feet – Open sight • 100 feet – Closed space (Steel Space)
	> 2 Mbps	5.5 Mbps	• 1100 feet – Open sight • 200 feet – Closed space (Steel Space)
	> 700 Kbps	1 Mbps	• 1200 feet – Open sight • 300 feet – Closed space (Steel Space)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.: Nº 189
Doc. 3698

Technical Specifications

Bluetooth MultiPort Module *(continued)*	**Usage Models** *(continued)*	**Access Point**:
		Corporate email, network neighborhood, access to LAN applications, file transfer, ftp, Internet browsing, etc, using TCP/IP
		Wireless link to WAN thru cell phone
		GSM/SMS, PCS, PHS, DECT, RAM, ARDIS, CDPD, etc.
		Agnostic to WAN technology
		Send/receive SMS messages
		Wireless link to Printer
		Adhoc peer to peer networking (two computers) or Personal Area Networking (PAN) using NDIS (< 7 computers)
		Adhoc Bluetooth Pico-networking (point to multi-point)
		Object Push – Business card or appointment exchange
	Transmit Power	< 20 dBM (Bluetooth Class 1)
	Receive Sensitivity	Better than –70 dBM at 0.1 % raw bit error rate
	Link Topology	Point to Point, Multipoint Pico Nets up to 7 slaves
	Security	Full support of Bluetooth Security Provisions
	Network Architecture Models	Ad-hoc (Peer to Peer)
		Infrastructure (Access Points Required)
	Power Requirement	Peak < 1500 mW
		Average < 500 mW
		Standby < 250 mW
	Power Management	Microsoft Windows ACPI, and USB Bus Support
		Keystrokes Fn+F2 Power On/Off control
		Self configurable to optimize power conservation in all operating modes, including Standby, Hold, Park, and Sniff
	OS Support	Microsoft Windows 2000
		Microsoft Windows XP Home
		Microsoft Windows XP Pro
	Protocols Supported	TCP/IP
		IPX/SPX
		UDP
	LED Activity	Solid Blue LED – On
		LED Off – Power Off
	Certifications	All necessary regulatory approvals for countries we support including:
		FCC (47 CFR) Part 15C, Section 15.247 & 15.249
		ETS 300 328, ETS 300 826
		Low Voltage Directive IEC950
		UL, CSA, and CE Mark

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. - Nº 190
Doc. 3698

Technical Specifications

Integrated 10/100 NIC	**NIC Device Driver Name**	RealTek (RTL 8139CL+).
	Data Link Layers	IEEE 802.2 LLC
		SNAP
	Ethernet Features	10 Mbps Ethernet: IEEE 802.3 standard 10BASE-T
		100 Mbps Ethernet: IEEE 802.3u standard 100BASE-TX
		Full Duplex at 10 and 100Mbps
		Auto-Negotiation
		Wake on LAN from standby
		Boot on LAN from OFF
		Lower Power State on Link Loss
	Software support	IBM LAN Server Version 1.2, 1.3, 2.0, 4.0
		Microsoft NT 3.51, NT 4.0. Microsoft Windows 2000
		Novell Netware 3.1x, 4.x, 5.x
	Protocol support	TCP/IP
		Novell IPX/SPX and Microsoft compatible
		Novel IPX ODI
		Microsoft NetBEUI
		IBM DLC

HP recommends Microsoft® Windows® XP Professional for Mobile Computing

©2003 Hewlett-Packard Corporation. All rights reserved. HP, the Compaq logo, Evo, Armada, Deskpro, iPAQ, and ProLiant are trademarks of hewlett-Packard Corporation. in the U.S. and/or other countries. Microsoft and Windows NT are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. Celeron, Intel, and Pentium, are registered trademarks or trademarks of the Intel Corporation in the U.S. and/or other countries. BatteryMark is a trademark of Ziff Davis Publishing Holdings Inc., and affiliate of eTesting Labs Inc., in the U.S. and other countries. All other product names mentioned herein may be trademarks of their respective companies.

HP shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

RQS nº 03/2005 - CN
CPMI - CORREIOS 23
Fls. Nº 191
3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 192
Doc. 3698

Technical Specifications

Type III Mini PCI 56K (V.92) **Modem**	**Form Factor**	Mini-PCI Type III per Specification
	Power Management Support	APM Revision 1.2, ACPI, Compaq Power Management Extensions for Microsoft Windows NT®
	Approvals/Certifications	UL, CSA, NEMKO, CCIB, Industry Canada, FCC Part 68, CTR21, FCC Part 15 Class B, Canadian ICES-003 Class B, C.I.S.P.R.22, Australian ACA, CE Mark, Other Countries
	Data Mode Capabilities	V.92 (a-law, mu-law)
		K56flex (a-law, mu-law)
		V.8bis
		V.80
		V44.bis, MNP5 (Compression)
		V42.bis, MNP5 (Compression)
		V.42 (LAPM, MNP2-4) (Error Correction)
		V.34 (file date: 10/96)
		Optional symbol rates:
		2800, 3429
		Asymmetric Symbol rates
		Synchronous primary channel data signaling rates:
		3600, 31200
		Automatic rate re-negotiation
		V.32bis
		V.32
		V.23
		V.22bis
		V.22
		V.21
		Bell 212A
		Bell 103J
	Fax Mode Capabilities	TIA-578-S (Class 1)
		T.30, T.4 (Group 3)
		V.17
		V.29
		V.27ter
		V.21 Channel 2
	Command Set	V.250 (Partial)
		TIA-602
		Identification: +GMI, +GMM, +GMR
		Port control: +IPR, +ICF, +IFC, +ILRR
		Modulation: +MS, +MR, +MA
		Error control: +ES, +ER, +EB, +ESR, +ETBM
		Data compression: +DS, +DR
		V.251

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 193
Doc. 3698

Technical Specifications

Bluetooth MultiPort Module	**Form Factor**	Compaq "MultiPort"	
	Bluetooth	1.1 Compliant	
	Dimensions	2.2 x 6.6 x 0.55 in (5.6 x 16.7 x 1.4 cm)	
	Weight	0.22 lb (100 g) (maximum)	
	Temperature	Operating	50° to 104°F (10° to 40°C)
		Non-operating	–4° to 140°F (–20° to 60°C)
	Humidity	Operating	10 to 90%
		Non-operating	5 to 95%
	Altitude	Operating	0 to 10,000 ft (3,048 m)
		Non-operating	0 to 30,000 ft (9,144 m)
	Plug and Play	USB 1.1 compliant	
		Microsoft Windows Plug and Play compliant	
	Frequency Band	2,4000 to 2.4835 GHz	
	Number of Available Channels	79 (1 MHz) available channels	
	Data Rates and throughput	1 Mbps	
		Synchronous Connection Oriented links up to 3, 64 kbps, voice channels	
		Asynchronous Connection Less links 723.2 kbps/57.6 kbps asymmetric or 433.9 kbps symmetric	
	Antenna type	Internally integrated within module (with special polarization diversity)	
	Range	328 ft/100 m	
	Profile Support	General Access Profile	
		Service Discovery Application Profile	
		Serial Port Profile	
		Generic Object Exchange Profile	
		File Transfer Profile	
		Synchronization Profile	
		Dial-Up Networking Profile	
		LAN Access Profile	
		Object Push Profile	
	Usage Models	Service Discovery (determine what Bluetooth devices are within range and support authorization)	
		Synchronization:	
		PDAs to PCs	
		Portable to Desktop	
		File Transfer:	
		File and directory browsing and navigation on another Bluetooth device.	
		File copying	
		Object manipulation – including add, delete, create new folders etc.	
		Wireless link to Corporate LAN using several Bluetooth devices sharing the same	

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 194
Doc. 3698

8427 A-

Technical Specifications

24X CD-ROM Drive	**Applicable Disk**	CD-ROM (Mode 1, 2 and 3), CD-XA ready (Mode 2, Form 1 and 2), CD-I ready (Mode 2, Form 1 and 2), CD-R (read only), CD Plus, Photo CD (Single and Multi-session), CD-Extra, Video CD, CD-WO (fixed packets only), CD-Bridge	
	Center Hole Diameter	0.59 in (15 mm)	
	Disk Diameter	12 cm, 8 cm	
	Disk Thickness	0.047 in (1.2 mm)	
	Track Pitch	1.6 µm	
	Access Times (typical reads, including settling)	Random	< 110 ms
		Full-Stroke	< 220 ms
	Audio Output Level	Line-out	0.7-0.9 Vrms
	Cache Buffer	128 KB	
	Data Transfer Rate (typical, including settling)	CD-ROM	3600 KB/s Maximum
	Start-up Time	< 10 seconds	
	Stop Time	< 5 seconds	
802.11b MultiPort Module	**Form Factor**	Compaq "MultiPort"	
	Weight	0.22 lb/100 g (maximum)	
	Operating Temperature	Operating	14° to 149° F (–10° to 65° C)
	Storage Temperature	Non-operating	–40° to 176° F (–40° to 80° C)
	Humidity	Operating	10 to 90%
		Non-operating	5 to 95%
	Altitude	Operating	0 to 15,000 ft (4,572 m)
		Non-operating	0 to 40,000 ft (12,192 m)
	Plug and Play	USB 1.1 compliant	
		Microsoft Windows Plug and Play compliant	
	RF Network Standard	IEEE 802 Part 11b (802.11b)	
	Frequency Band	2,4000 to 2.4835 GHz	
		2,4465 to 2.4835 GHz (France)	
		2,4000 to 2,4697 GHz (Japan)	
	Number of Selectable Sub-channels	**Worldwide Certification**	
		United States (FCC)	11
	Data Rates	1, 2, 5.5, 11 Mbps	
	Antenna type	Internally integrated within module (with special polarization diversity)	
	WEP Security	64-bit encryption keys compliant to IEEE 802.11	
		128-bit encryption key compliant to IEEE 802.11	
		Ability to enter keys manually or via pass-phrase	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 195
Doc. 3698

8429
9-

Technical Specifications

Diskette Drive	**Diskette Size**	3.5 in	
	Activity Indicator	On system	
	Height	0.5 in (12.7 mm)	
	Bytes per Sector	512	
	Sectors per track	High density	18 (1.44 MB)/15 (1.2 MB)
		Low density	9
	Tracks per side	High density	80 (1.44 MB)/80 (1.2 MB)
		Low density	80
	Read/Write heads	2	
	Access Times	Track-to track (high/low)	3 ms/6 ms
		Average (high/low)	94 ms/174 ms
		Settling time	15 ms
		Latency average	100 ms
External AC Adapter	**Weight**	0.85 lb (0.385 kg)	
	Power Supply (Input)	Operating Watts	90
		Operating Voltage	110 to 240 VAC RMS
		Operating Current	1.5 A RMS
		Operating Frequency Range	50 to 60 Hz AC
Lithium-Ion Battery Pack (8-cell)	**Dimensions** (L x W x D)	4.95 x 3.46 x 0.8 in (12.5 x 8.8 x 2 cm)	
	Weight	0.96 lb (0.43 kg)	
	Energy	Voltage	14.8 V
		Amp-hour capacity	Minimum 3.7 Ah Typical 3.9 Ah
		Watt-hour capacity	Minimum 53.2 Ah Typical 56.1 Ah
	Temperature	Operating	32° to 108° F (0° to 42° C)
		Non-operating	32° to 140° F (0° to 60° C)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 196
Doc. 3698

8431
A.

Technical Specifications

Hard Drives

60-GB	**Capacity**	60 GB	
	Drive Weight	0.34 lb (155 g)	
	Height	0.374 in (9.5 mm)	
	Width	70 mm	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	2.5 ms
		Average	13 ms
		Maximum	23 ms
	Rotational Speed	5400 rpm	
	Logical Blocks	117,210,240	
	Operating Temperature	41° to 131° F (5° to 55° C)	
	Features	Security	ATA Security
40-GB	**Drive Weight**	0.21 lb (95 g)	
	Capacity	40 GB	
	Height	0.374 in (9.5 mm)	
	Width	2.75in (70 mm)	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	3.0 ms
		Average	13 ms
		Maximum	25 ms
	Rotational Speed	4200 rpm	
	Logical Blocks	78,140,160	
	Operating Temperature	41° to 131° F (5° to 55° C)	

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 197
Doc. 3698

Technical Specifications

System Unit	**Dimensions** (H x W x D)	15-inch and 14.1-inch TFT panel displays	1.55 x 12.89 x 10.53 in (3.95 x 32.75 x 26.75 cm)
	Weight With P4 processor	14 inch: LCD, DVD or CD-ROM, 1 SODIMM	6.82 lb (3.1 kg)
		15 inch LCD, DVD or CD-ROM, 1 SODIMM	7.09 lb (3.2 kg)
	Weight With Celeron processor	14 inch: LCD, DVD or CD-ROM, 1 SODIMM	6.60 lb (3 kg)
		15 inch LCD, DVD or CD-ROM, 1 SODIMM	6.87 lb (3.12 kg)
	NOTE: * = Weight varies by configuration.		
	Stand-Alone Power Requirements	Nominal Operating Voltage (Li-Ion)	14.4 V (8-cell)
		Average Operating Power	29.7 W Desktop
		Peak Operating Power	80 W on AC
			55 W on DC
		Power in suspend mode	< 1000 mW
		Power in hibernation mode	< 100 mW
	Power Supply	Rated Input Voltage	100 to 240 VAC
		Rated Input Current	< 1.5 A
		Rated Frequency	50 to 60 Hz
	Temperature	Operating	50° to 95° F (10° to 35° C)
		Non-operating	14° to 140° F (–10° to 60° C)
	Relative Humidity	Operating	10% to 90% relative humidity, non-condensing
		Non-operating	5% to 90% relative humidity, 101.6° F (38.7° C) Maximum wetbulb temperature
	Shock	Operating	10 G, 11 ms, half-sine
		Non-operating	60 G, 11 ms, half-sine
	Vibration	Operating	0.5 G zero-to-peak, 10 to 500 Hz, 0.25 oct/min sweep rate
		Non-operating	1.0 G, zero-to-peak, 10 to 500 Hz, 0.5 oct/min sweep rate
	Maximum Altitude (unpressurized)	Operating	0 to 10,000 ft (0 to 3,048 m)
		Non-operating	0 to 30,000 ft (0 to 9,144 m)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 198
3698
Doc.

Memory

Compaq Evo N1020V

STANDARD MEMORY PLUS OPTIONAL MEMORY

Support for up to 1024 MB of DDR SDRAM memory is available with the installation of optional DDR SDRAM Memory Kits.

Memory	Slot 1	Slot 2
256 MB	256 MB	–
384 MB	256 MB	128 MB
512 MB	512 MB	–
768 MB	512 MB	256 MB
1024 MB	512 MB	512 MB

NOTE: This chart does not represent all possible memory configurations. Due to the non-industry standard nature of some third-party memory modules, we strongly recommend using only Compaq branded memory modules to ensure compatibility.

Following are memory options available from Compaq:

• 512-MB (266 MHz) Memory Upgrade	269087-B25
• 256-MB (266 MHz) Memory Upgrade	269086-B25
• 128-MB (266 MHz) Memory Upgrade	269085-B25

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 199
Doc. 3698

8437 A

Options

Memory	512-MB (266 MHz) Memory Upgrade		269087-B25
	256-MB (266 MHz) Memory Upgrade		269086-B25
	128-MB (266 MHz) Memory Upgrade		269085-B25
Monitors	TFT8030 Flat Panel Color 18-inch (carbon/silver)		243362-001
	TFT7020 Flat Panel Color 17-inch with integrated speakers (carbon/silver)		253217-001
	TFT5015 Flat Panel Color 15-inch (carbon/silver)		234044-001
	TFT5030 Flat Panel Color 15-inch (carbon/silver)		228134-001
	V720 17-inch CRT (carbon/silver)		232944-001
	S720 17-inch CRT (carbon/silver)		239287-001
	V570 15-inch CRT (carbon/silver)		228113-001
Other Storage Devices	IBM 1-GB Microdrive (PC card Device)		217390-B25
	USB 32-MB DiskOnKey		301993-B21
Connectivity	Compaq Type II Mini PCI 56K (V.90) Modem		225640-B31
	Compaq Type II Mini PCI 56K (V.90) Modem plus 10/100 NIC Combo		225642-B31
	100BaseTX Ethernet Upgrade		225435-001
	1394 PC Card		177593-B25
	NOTE: Designed only to allow faster downloads from V.90 compliant sources. Maximum achievable download transmission rates currently do not reach 56 KB/s, and will vary with line conditions.		
Wireless Connectivity	802.11b MultiPort Wireless LAN module		283836-001
	Bluetooth MultiPort module		228057-B21
	Compaq WL110 Wireless LAN PC Card		191808-001
	Compaq WL510 Wireless Enterprise Access Point		216709-001
	Compaq WL410 Wireless SMB Access Point		191811-001
	Compaq WL310 Home Office Access Point		191813-001
	Compaq Range Extender Antenna		230268-B21
	CDPD WWAN PC Card (U.S. Only)		238111-001
Expansion Bases	Port Replicator		307648-001
	Advanced Port Replicator		307651-001
	External MultiBay		217388-001/002
	Monitor Stand		274407-B25
Power	Evo Notebook N1020v	8 Cell primary battery (4 Ah)	278418-B25
		8 Cell primary battery (4.4 Ah)	291369-B25
Common Power Solutions	External Battery Charger		265603-001
	External Battery Charger (Multiple Battery)		265604-001
	AC Adapter (90W)		283884-001
	Aircraft Power Adapter (90W)		291370-B25

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 200
Doc. 3698

Standard Features

MODELS

N1020vC160X420DC25E *P/N 470045-646*	**Display**	14.1-inch color TFT XGA
	Processor	1.60 GHz Celeron
	Cache Memory	256 KB, L2 Cache
	Standard Memory	256 MB (1 DIMM) 266 MHz DDR
	Maximum Memory	1024 MB (266 MHz) DDR
	Hard Drive	20 GB
	Optical Drive	24X CD-ROM Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Home
	Warranty	One Year
N1020vP200X430VC25O *P/N 470045-647*	**Display**	14.1-inch color TFT XGA
	Processor	2.0 GHz Intel Pentium 4 processor
	Cache Memory	512 KB, L2 Cache
	Standard Memory	256 MB (1 DIMM) 266 MHz DDR
	Maximum Memoru	1024 MB (266 MHz) DDR
	Optical Drive	30 GB
	Hard Drive	8X DVD-ROM Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Pro
	Warranty	One Year
N1020vP240X540WC25O *P/N 470045-648*	**Display**	15-inch color TFT XGA
	Processor	2.4 GHz Intel Pentium 4 processor
	Cache Memory	512 KB, L2 Cache
	Standard Memory	256 MB (1 DIMM) 266 MHz DDR
	Maximum Memoru	1024 MB (266 MHz) DDR
	Optical Drive	40 GB
	Hard Drive	DVD/CD-RW Combo Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Pro
	Warranty	One Year

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 201
Doc. 3698

Standard Features

Security	Configuration Control Hardware Memory Change Alert Ownership Tag Set-up Password Power-On Password DriveLock Enabled for PC SmartCard options Kensington Lock
Power Supply	External 90-watt AC adapter, power cord included.
Battery	Standard 8-cell Lithium-Ion battery. The Evo Notebook N1020v provides over two hours of battery life using the standard 8-cell Lithium-Ion battery. **NOTE**: Actual results may vary with product model, configuration, and individual usage. Compaq results of 2:20 (hr:min) were achieved running the Business Winstone 2001 Battery Mark™ 1.0 on a N1020Vv with a Intel Pentium 4 2.0 GHz CPU, 15-inch XGA panel, 256-MB RAM, 30-GB HDD, 8X DVD, 8-cell Lithium-Ion battery, and NIC/modem. System parameters were set according to eTesting Labs' recommendations: panel brightness 50%, hard drive timer three minutes. **NOTE**: This test was performed without independent verification by eTesting Labs Inc. eTesting Labs Inc. makes no representations or warranties as to the result of the test. BatteryMark is a trademark of Ziff Davis Publishing Holdings Inc., and affiliate of eTesting Labs Inc., in the U.S. and other countries.
Power Conservation	Hibernation Instant-on via Standby Pop-ups with three presets One custom level of power conservation ACPI compliant
MultiPort	MultiPort is a flexible, innovative solution providing customers the ability to connect to their choice of wireless standards such as 802.11b or Bluetooth™. This can be achieved by simply changing out the high-performance wireless module, which is integrated into the top of the notebook. The award-winning MultiPort offers a cost effective means to migrate to future wireless standards as they become available.
Docking	Port replicator and Advanced Port Replicator. The sleek, new port replicator and advanced port replicator designs provide simple and convenient port management. Features include NIC pass through, USB, and a 1394 digital port. Compatible across multiple platforms for lower total cost of ownership.
Service and Support	Compaq Services includes a one-year, Worldwide Limited Warranty, pick-up or carry-in; upgraded warranty and toll-free 7 x 24 hardware technical phone support available. **NOTE**: Certain restrictions and exclusions apply. Consult the Compaq Customer Support Center for details.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 202
Doc. 3698

Standard Features

Processor and Panel	15-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal) 14.1-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal)	
One of the following:	2.4 GHz Intel Pentium 4 processor with 512 KB L2 cache 2.0 GHz Intel Pentium 4 processor with 512 KB L2 cache 1.6 GHz Intel Celeron with 256 KB L2 cache	
Memory	Standard/Maximum	256 MB (266 MHz) DDR SDRAM (256 MB SODIMM in slot 1) 576 1024 MB (266 MHz) DDR SDRAM (512 MB SODIMMs in slots 1 and 2)
	NOTE: Due to the non-industry standard nature of some third-party memory modules, we recommend Compaq branded memory to ensure compatibility.	
Communications	10/100 NIC is integrated on the system board Type III Mini PCI 56K (V.92) modem **NOTE**: Designed only to allow faster downloads from V.92 compliant sources. Maximum achievable download transmission rates currently do not reach 56 KB/s, and will vary with line conditions. **NOTE**: Modem availability is subject to country regulatory approval	
Keyboard	88-key compatible keyboard with isolated, inverted-T cursor control keys, special feature hotkeys for instant access to power conservation, toggle between internal and external, or simultaneous displays, and control brightness and contrast.	
Easy Access Internet Buttons	The Evo Notebook N1020V comes with three Easy Access Buttons (EAB) designed to increase customer productivity by providing one-touch access to helpful Compaq information, favorite Internet destinations, or default e-mail application. The EAB portion of the keyboard deck also includes dedicated hardware volume control and a quick-launch button for CD/DVD play.	
Pointing Device	Touchpad with 4-way scroll	
PC Card Slots	One Type II PC Card Slot which supports both 32-bit CardBus and 16-bit PC Cards	
Storage	Fixed Diskette Drive	1.44-MB Diskette Drive
	Primary Hard Drive	40 GB or 30 GB or 20 GB
	Fixed Optical Drive	DVD/CD-RW Combo Drive DVD-ROM Drive CD-ROM Drive

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 203
3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3004
Doc. 3698

8421
A.

QuickSpecs

HP PS/2 Scroll Mouse

MODELS

Compaq PS/2 Scroll Mouse (Carbon)
DC171A

HP PS/2 Scroll Mouse (Carbonite)
DD440B

OVERVIEW

The HP PS.2 Scroll Mouse is a two-button mouse that offers great wheel mouse performance in a simple, elegant design. Use the wheel for fast and easy scrolling in documents or on the Web, or as a third button. The HP PS/2 Scroll Mouse's comfortable, contoured shape fits either right or left hand.

Key Benefits

- Comfortable design fits either hand
- Wheel permits easy scrolling, functions as third button
- Speeds document navigation on the Web

COMPATIBILITY

The Compaq PS/2 Scroll Mouse (Carbon) is compatible with Compaq Evo D300 and D500 series PCs (except the Compaq Evo D510 e-pc). The HP PS/2 Scroll Mouse (Carbonite) is compatible with HP Compaq Business Desktop d220, d230, d330 and d530 Series PCs, the HP Business Desktop d325 Microtower and HP Workstations xw4000, xw5000, xw6000, and xw8000.

SERVICE AND SUPPORT

The HP PS/2 Scroll Mouse has a one-year limited warranty or the remainder of the warranty of the HP product in which it is installed. Technical support is available seven days a week, 24 hours a day, by phone as well as in online support forms. Certain restrictions and exclusions apply.

SPECIFICATIONS

Dimensions	3.8 x 6.3 x 11.6 cm (1.5 x 2.5 x 4.6 in)	
Weight	4.44 oz (126 g)	
Environmental	**Operating temperature**	50 to 122 °F (10 to 50 °C)
	Non-operating temperature	–22 to 140 °F (–30 to 60 °C)
	Operating humidity	10% to 90% (non condensing at ambient)
	Non-operating humidity	20% to 80% (non condensing at ambient)
	Operating shock	40 g, 6 surfaces
	Non-operating shock	80 g, 6 surfaces
	Operating vibration	2 g peak acceleration
	Non-operating vibration	4 g peak acceleration
	Drop (out of box)	26 in (66 cm) on carpet, 6-drop sequence
	Drop (out of box)	1 m on asphalt tile over concrete, 6-drop sequence
Electrical	**Operating voltage**	5 VDC ± 10%
	Power consumption	15 mA
	System consumption	PS/2 mini-din connector
	ESD	CE level 4, 15 kV air discharge
	EMI-RFI	Conforms to FCC rules for a Class B computing device
	Microsoft PC99 - 2001	Functionally compliant

invent

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 205
3698
Doc.

SPECIFICATIONS *(continued)*

Mechanical	**Resolution**	400 ± 20% DPI
	Tracking speed	10 in/s (25.4 cm/s) maximum
	Acceleration	100 in/s/s (2.54 m/s/s)
	Switch actuation	65 g nominal peak force
	Switch life	1,000,000 operations (using Hasco modified tester)
	Switch type	Low force micro-switches
	Tracking mechanism life	155 mi (250 km) at average speed of 10 in/s
	Cable length	6 ft (1.8 m)
	Microsoft PC99 - 2001	Mechanically compliant
Scroll wheel	**Width**	8 mm
	Diameter	25.2 mm (.99 in)
	Maximum rotation speed	30 mm/s
	Switch type	Light force micro-switch
	Switch life	1 million operations
	Mechanical life	Minimum 200,000 revolutions
Regulatory approvals	**Compliant**	UL, CSA, FCC, CE Mark, TUV, TUV GS, VCCI, BSMI, C-Tick, MIC
Compatibility	**Operating system support**	Microsoft® Windows Me, Windows 2000 and Windows XP

HP recommends Microsoft® Windows® XP Professional for Business

© 2003 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 206
Doc. 3698

8419 A.

QuickSpecs

hp *CRT monitor s7500*

Overview

Models	**HP CRT monitor s7500** *261606-xxx*

TECHNICAL SPECIFICATIONS

Tube Type	Color, Conventional FST, multi-frequency				
Picture Tube Size (diagonal)	17- nch (43.18 cm)				
Viewable Image Area (diagonal)	16-inch (40.64 cm)				
Trio Dot Pitch	0.28 mm				
Horizontal Dot Pitch	0.24 mm				
Horizontal Frequency (kHz)	30 to 70 kHz				
Vertical Frequency (Hz)	50 to 140 Hz				
Maximum Pre-set Resolution	1280 x 1024 @ 60 Hz				
Preferred Flicker Free Resolution	1024 x 768 @ 85 Hz				
Preset Graphic Modes	1280 x 1024	1024 x 768	800 x 600	720 x 400	640 x 480
NOTE: All modes are non-interlaced unless specified otherwise	@ 60 Hz	@ 85 Hz and 75 Hz	@ 85 Hz and 75 Hz	@ 70 Hz	@ 85 Hz, 75 Hz, 60 Hz
User-Modes	Yes, 8 modes				
Anti-Glare/Anti-Static	Yes				
AssetControl	Yes, supported				
Plug and Play	Yes				
Icon Based On-Screen Display Controls	Yes				

User Controls	**Brightness, Contrast**	Yes
	Size and Positioning	Yes
	Pincushion (barrel)	Yes
	Trapezoid	Yes
	Tilt (rotation)	Yes
	Selectable Color temperature	Yes
	Parallelogram	Yes
	Pincushion Balance	Yes
	Exit	Yes
	Degauss	Yes
	Factory Reset/Recall	Yes
	Current Display Mode	Yes

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 207
3698
Doc.

TECHNICAL SPECIFICATIONS *(continued)*		
Approvals/Certifications	**UL/CSA/CUL Approval**	Yes
	ISO9241-3, -7, -8 VDT Guidelines Approval	Yes
	MPR-II Compliant	Yes, select models
	TCO '99	Yes, select models
	FCC Approval	Yes
	Microsoft WHQL Certified	Yes
	Energy Star Compliant	Yes
	CE	Yes
Maximum Pixel Clock Speed	110 MHz	
Power Supply	Universal; 100 to 240 V, 50 ± 3Hz and 60 ± 3Hz	
Maximum Power Rating	≤ 100 watts	
Low Power Sleep Mode	< 5 watts	
Signal Cable	15-pin miniature D-sub, attached, 4.9 feet (1.5 meters)	
Dimensions (H x W x D)	**Unpacked**	17 x 16.6 x 17.5 in (43.2 x 41 x 44.5 cm)
	Packaged	18.9 x 20.3 x 22.1 in (48 x 51.6 x 56.1 cm)
Weight	**Unpacked**	38 lb (17.23 kg)
	Packaged	46.2 lb (20.9 kg)
Operating Temperature (non-condensing)	50° to 95°F (10° to 35°C)	
Operating Humidity non-condensing)	20% to 80%	
Compatibility	Compaq Evo PCs and Thin Clients and Compaq D315 Business PC	
Warranty	Limited three-year parts and repair labor, one-year Service Provider labor and one-year on-site service warranty. 48 hour advanced exchange service available during warranty period. Certain restrictions and exclusions apply. For details, contact HP Customer Support.	

©2003 Hewlett-Packard Development Company, L.P. The information in this document is subject to change without notice and is provided "as is" without warranty of any kind. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 208
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 209
Doc. 3698

8437
A.

QuickSpecs

hp *CRT monitor s7500*

Overview

Models	**HP CRT monitor s7500**	*261606-xxx*

TECHNICAL SPECIFICATIONS

Tube Type	Color, Conventional FST, multi-frequency				
Picture Tube Size (diagonal)	17- nch (43.18 cm)				
Viewable Image Area (diagonal)	16-inch (40.64 cm)				
Trio Dot Pitch	0.28 mm				
Horizontal Dot Pitch	0.24 mm				
Horizontal Frequency (kHz)	30 to 70 kHz				
Vertical Frequency (Hz)	50 to 140 Hz				
Maximum Pre-set Resolution	1280 x 1024 @ 60 Hz				
Preferred Flicker Free Resolution	1024 x 768 @ 85 Hz				
Preset Graphic Modes	1280 x 1024	1024 x 768	800 x 600	720 x 400	640 x 480
NOTE: All modes are non-interlaced unless specified otherwise.	@ 60 Hz	@ 85 Hz and 75 Hz	@ 85 Hz and 75 Hz	@ 70 Hz	@ 85 Hz, 75 Hz, 60 Hz
User-Modes	Yes, 8 modes				
Anti-Glare/Anti-Static	Yes				
AssetControl	Yes, supported				
Plug and Play	Yes				
Icon Based On-Screen Display Controls	Yes				
User Controls	**Brightness, Contrast**	Yes			
	Size and Positioning	Yes			
	Pincushion (barrel)	Yes			
	Trapezoid	Yes			
	Tilt (rotation)	Yes			
	Selectable Color temperature	Yes			
	Parallelogram	Yes			
	Pincushion Balance	Yes			
	Exit	Yes			
	Degauss	Yes			
	Factory Reset/Recall	Yes			
	Current Display Mode	Yes			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 210
3698
Doc.

TECHNICAL SPECIFICATIONS *(continued)*		
Approvals/Certifications	**UL/CSA/CUL Approval**	Yes
	ISO9241-3, -7, -8 VDT Guidelines Approval	Yes
	MPR-II Compliant	Yes, select models
	TCO '99	Yes, select models
	FCC Approval	Yes
	Microsoft WHQL Certified	Yes
	Energy Star Compliant	Yes
	CE	Yes
Maximum Pixel Clock Speed	110 MHz	
Power Supply	Universal; 100 to 240 V, 50 ± 3Hz and 60 ± 3Hz	
Maximum Power Rating	≤ 100 watts	
Low Power Sleep Mode	< 5 watts	
Signal Cable	15-pin miniature D-sub, attached, 4.9 feet (1.5 meters)	
Dimensions (H x W x D)	**Unpacked**	17 x 16.6 x 17.5 in (43.2 x 41 x 44.5 cm)
	Packaged	18.9 x 20.3 x 22.1 in (48 x 51.6 x 56.1 cm)
Weight	**Unpacked**	38 lb (17.23 kg)
	Packaged	46.2 lb (20.9 kg)
Operating Temperature (non-condensing)	50° to 95°F (10° to 35°C)	
Operating Humidity non-condensing)	20% to 80%	
Compatibility	Compaq Evo PCs and Thin Clients and Compaq D315 Business PC	
Warranty	Limited three-year parts and repair labor, one-year Service Provider labor and one-year on-site service warranty. 48 hour advanced exchange service available during warranty period. Certain restrictions and exclusions apply. For details, contact HP Customer Support.	

©2003 Hewlett-Packard Development Company, L.P. The information in this document is subject to change without notice and is provided "as is" without warranty of any kind. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 211
3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 212
Doc. 3698

Technology Foundation

IBM WebSphere

The Issue: Meeting Business Objectives in an e-Business World

To create an effective e-business infrastructure, you need more than a Web interface for your J.D. Edwards applications. You need a solid Web infrastructure that is dependable, scalable, and robust enough to handle fluctuating transaction volumes without missing a beat. The infrastructure must also include integrated development tools that allow you to keep your technology solution in line with changing business requirements. Above all, it must be able to meet your current and future enterprise application requirements—right out of the box.

The Solution: WebSphere® Application Server for J.D. Edwards Web Implementations

J.D. Edwards offers the complete end-to-end solution to Web enable your J.D. Edwards applications—J.D. Edwards Technology Foundation. IBM's WebSphere Application Server Advanced Edition 4.0 is bundled with the Technology Foundation to provide the ideal platform for your J.D. Edwards Web applications. Together, the WebSphere Application Server and J.D. Edwards' Web-enabled applications create a comprehensive, enterprise-class solution that offers flexibility, scalability, security, ease of use, and a lower total cost of ownership, while supplying you with industry-leading functionality and performance.

Tightly integrated with sophisticated development tools, the WebSphere Application Server provides advanced integration capabilities based on open, industry-standard technologies. It allows you to leverage existing IT assets by connecting to a variety of databases and platforms.

With the WebSphere Application Server, you are able to:

- Make changes in application logic without reworking code, even while the application is running.
- Efficiently share dynamic customer information from one end of a distributed application to the other.
- Deploy applications based on the Java 2 Platform, Enterprise Edition (J2EE) standard that intelligently adjust presentation and business logic for different client locales and time zones.
- Increase availability by scaling through horizontal or vertical cloning.
- Integrate enterprise information systems as reusable business services.
- Connect with existing Microsoft®, Common Object Request Broker Architecture (CORBA), and C++ applications.
- Handle business events through advanced messaging technology.

Feature/Function Highlights

- J2EE compliance
- Java technology foundation
- Firewall support
- Browser-based administration tools
- Internationalization services
- Extended messaging support
- Built-in process engine
- Business rules support
- Shared work areas
- Bidirectional CORBA connectivity
- C++ CORBA software developer's kit
- ActiveX bridge
- High-speed transaction processing support

Platform Operating Systems Support

- AIX 4.3.3 and 5.1
- HP-UX 11.0 and 11i (or 11.11)
- Solaris 7 and 8
- Windows 2000 SP3 and Advanced Server SP3
- AS/400 V5R1 and V5R2

JDEDWARDS

you > us

www.jdedwards.com

Fls. Nº 213
Doc. 5608

Lower Your Total Cost of Ownership

As part of the J.D. Edwards Technology Foundation, the WebSphere Application Server offers a cost-effective and efficient way for you to deploy J.D. Edwards applications.

By purchasing the WebSphere Application Server as part of the J.D. Edwards Technology Foundation, you save time and money through application pre-integration. And with J.D. Edwards as your complete solution vendor, you benefit from further cost savings by having a single source for service and support, rather than having multiple vendors.

The WebSphere Application Server also saves costs by simplifying administration and systems management. It provides a central and open management interface to help you administer multiple applications and components from the same environment. Built-in set-up options and administrative features aid in application deployment and administration, while automated management functions enhance productivity and reduce administrative costs.

Enhance Flexibility

With multiple configuration options, the WebSphere Application Server supports a wide range of scenarios, from simple administration of a single server to a clustered, high-availability, high-volume environment. The specialized configuration options give you the flexibility to respond to an ever-changing market—without the costs of migrating to a different technology base.

Support Enterprise Needs

With J.D. Edwards and the WebSphere Application Server, you are able to extend your enterprise applications to the Web, efficiently and cost effectively. With scalability built in—through such capabilities as cloning, for example—the WebSphere Application Server can be used in a variety of environments. To help in large installations, J.D. Edwards' customers can take advantage of the IBM EdgeServer*. By supporting dynamic load balancing between physical Web servers, it is ideal for larger enterprise environments.

With the WebSphere Application Server, you benefit from a flexible infrastructure that offers unmatched functionality and stability and is easy to deploy and support. Delivered by two industry leaders, the WebSphere Application Server, as part of the Technology Foundation, is built to support your business needs.

J.D. Edwards: A Strategic Partner for Your Long-term Needs

A solution is only as good as the company that stands behind it. That is why J.D. Edwards is committed to innovation, superior value, and customer satisfaction. Our singular goal is to help make you stronger, enabling you to solve your most important business challenges. We do this by dedicating ourselves to continually enhancing the value of our solutions, not only with software research and development, but also with superior consulting, education, and training support. As your long-term business partner, J.D. Edwards will work with you to help ensure that our solutions grow and change with your business—making your technology investment an asset that increases in value over time.

*EdgeServer is not included in the J.D. Edwards Technology Foundation product offering, but is available through IBM or an IBM channel reseller.

Database Support

- UNIX
- UDB 7.2 FP 5 or 7
- Oracle 8.1.7.3 or 4 and 9.0.1.4
- Windows
- UDB 7.2 FP 5 or 7
- Oracle 8.1.7.3 or 4 and 9.0.1.4
- SQL 2000 SP3
- AS/400 DB2 for iSeries

Solution Integration

- ERP
- CRM
- Supply Chain Management
- Supplier Relationship Management
- Business Intelligence
- Collaborative Portal

J.D. Edwards
World Headquarters
One Technology Way
Denver, Colorado 80237, USA
800 727 5333 / 303 334 4000
www.jdedwards.com

J.D. Edwards (UK) Ltd.
Europe, the Middle East, and Africa
Colorado House
300 Thames Valley Park Drive
Reading
Berkshire RG6 IRD, UK
044 1189 091 700
www.jdedwards.co.uk

J.D. Edwards
Latin America and the Caribbean
806 Douglas Entrance, Suite 570
Coral Gables, Florida 33134, USA
305 442 7800
www.jdedwards.com.mx

J.D. Edwards (Asia Pacific) Pte Ltd.
No. 1 International Business Park
The Synergy, #06-01/04
Singapore 609917
65 227 3391
www.jdedwards.com.tw

March 2003

The materials contained herein are summary in nature, subject to change, and intended for general information only. J.D. Edwards® is a registered trademark of J.D. Edwards & Company. JDE™ is a trademark of J.D. Edwards & Company. J.D. Edwards 5 is a trademark of J.D. Edwards World Source Company. The names of all products and services of J.D. Edwards used herein are trademarks or registered trademarks of J.D. Edwards World Source Company. All other product names used herein are trademarks or registered trademarks of their respective owners. © J.D. Edwards World Source Company 2003. U.S. and/or Canadian patents and patent applications may cover inventions used in the production of J.D. Edwards 5.

WASpss.0303

Fls. Nº 214
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 215
Doc. 3698

8413
A.

Oracle9*i* Database Release 2 Product Family

An Oracle White Paper

June 2003

ORACLE

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc. 3698

any edition of Oracle9*i* Database will run with the others, although Oracle9*i* Enterprise Edition provides additional performance, scalability, availability and security functions that are generally transparent to application developers. The APIs supported with Oracle9*i* Enterprise Edition are generally also supported with Oracle9*i* Personal Edition and Oracle9*i* Standard Edition, with exceptions related to the functionality associated with optional additional products only available with Oracle9*i* Personal Edition and Oracle9*i* Enterprise Edition such as Oracle OLAP or Oracle Data Mining.

These Oracle9*i* Database products are all built using the same robust and reliable database engine architecture. Oracle9*i* Database Standard Edition and Oracle9*i* Database Personal Edition are both 100 percent compatible with Oracle9*i* Database Enterprise Edition on many different platforms, so your database applications can scale from the laptop to the desktop to the enterprise without re-engineering.

As your business grows over time, you can easily upgrade from the Oracle9i Database Standard Edition to the Enterprise Edition as your business requires more scalability and functionality. One of the benefits of Oracle SE is that it's so easy to upgrade to EE -- just install the EE software -- you make *no* changes to your database, application, or administrative procedures, and you get all the additional reliability, availability, scalability, and other benefits of EE.

ADVANCED OPTIONS TO MEET DEMANDING REQUIREMENTS

The three Oracle9*i* Database products each have features and functionality to meet the varying requirements of today's applications. Additionally, Oracle offers optional products that contain sophisticated technology to meet your most demanding requirements for development and deployment of mission-critical OLTP, data warehouse, and Internet application environments.

Oracle Real Application Clusters

Oracle Real Application Clusters provides unlimited scalability and high availability for any packaged or custom application by exploiting clustered hardware configurations, with the simplicity and ease of use of a single system image. Oracle Real Application Clusters allows access to a single database from multiple nodes of a clustered system configuration, to insulate application and database users from hardware and software failures, while providing performance that scales with the hardware environment.

Oracle Partitioning

Oracle Partitioning enhances the data management environment for OLTP, data mart, and data warehouse applications by adding significant manageability, availability, and performance capabilities to large underlying database tables and indexes. Oracle Partitioning permits large tables to be broken into individually managed smaller pieces, while retaining a single application-level

ECT nº 03/2005 - CN
CPMI - CORREIOS
217
Fls. Nº
Doc. 3698

vendor tools and applications to access spatial data directly from Oracle9*i* Database, providing interoperability and minimizing costs.

Oracle Enterprise Manager Packs

In addition to Oracle Enterprise Manager, Oracle provides an advanced integrated package of tools for performance tuning, diagnostics, and change management:

- *Oracle Tuning Pack* - Oracle Tuning Pack provides database administrators with expert performance management for the Oracle environment, including SQL tuning and storage optimization.
- *Oracle Diagnostics Pack* - Oracle Diagnostics Pack enables database administrators to perform advanced monitoring, diagnosis, and planning for the Oracle environment.
- *Oracle Change Management Pack* - Oracle Change Management Pack eliminates errors and loss of data when upgrading databases to support new applications. The pack analyzes the impact and complex dependencies associated with application change and automatically performs database upgrades.
- *Oracle Management Pack for SAP R/3* - Oracle Management Pack for SAP R/3 offers real time monitoring for SAP R/3 systems, capacity planning for historical analysis and future planning purposes, event integration, and a single point of administration of the host, database, and application.

Oracle Programmer

Oracle Programmer is a product that provides a rich set of interfaces for developers who build enterprise applications that access and manipulate Oracle9*i* database.

Oracle Programmer is a family of products consisting of:

- Three embedded SQL-style interfaces: Precompilers, SQL*Module, and SQLJ
- Four call level interfaces: Oracle Call Interface (OCI), Oracle C++ Call Interface (OCCI), ODBC, and JDBC
- Two COM data access interfaces: Oracle Objects for OLE and Oracle Provider for OLE DB
- Microsoft .Net support: Oracle Data Provider for .NET (ODP.NET), OLE DB .NET, and ODBC .NET
- Two utilities to generate host-language bindings from database schemas: Object Type Translator and JPub

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 218
Doc. 3698

8407
A.

Transparent application failover	N	Y	
Scalability			
Oracle Real Application Clusters	N	Y	Extra cost option
Cluster File System	N	Y	Requires RAC
Java native compilation	Y	Y	
PL/SQL native compilation	Y	Y	
Security			
Advanced Security Option	N	Y	Extra cost option
Oracle Label Security	N	Y	Extra cost option
Encryption toolkit	Y	Y	
Virtual Private Database	N	Y	
Fine grained auditing	N	Y	
DBA auditing	Y	Y	
Password management	Y	Y	
Proxy authentication	Y	Y	
Development Platform			
Oracle Programmer	Y	Y	Extra cost product
Java support	Y	Y	
SQLJ	Y	Y	Requires Oracle Programmer
JDBC drivers	Y	Y	
XML DB	Y	Y	
Objects and extensibility	Y	Y	
PL/SQL stored procedures and triggers	Y	Y	
PL/SQL Server Pages	Y	Y	
User-defined aggregates	Y	Y	
COM Automation Feature	Y	Y	Windows only

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 219
3698
Doc.

8405
A-

Database Resource Manager	N	Y	
Oracle Managed Files	Y	Y	
Locally Managed Tablespaces	Y	Y	
Resumable space allocation	Y	Y	
Unused index identification	Y	Y	
VLDB, Data Warehousing, Business Intelligence			
Oracle Partitioning	N	Y	Extra cost option
Oracle OLAP	N	Y	Extra cost option
Oracle Data Mining	N	Y	Extra cost option
Data Compression	N	Y	
Optimizer statistics management	Y	Y	
Analytic functions	Y	Y	
Bitmapped index and bitmapped join index	N	Y	
Descending index	Y	Y	
Function-based index	Y	Y	
Automated parallel query degree	N	Y	
Parallel statistics gathering	N	Y	
Parallel bitmap star query optimization	N	Y	
Parallel DML	N	Y	No longer requires Partitioning option
Parallel index build	N	Y	
Parallel index scans	N	Y	
Parallel load	Y	Y	
Parallel query	N	Y	
Star query optimization	Y	Y	
Sample scan	Y	Y	

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 220
3698
Doc.

8403
A.

Oracle Net Services	Y	Y	
Content Management			
Oracle Spatial	N	Y	Extra cost option
Dynamic Services	Y	Y	
Oracle Database Workspace Manager	Y	Y	
Parallel text index creation	N	Y	
Ultra Search	Y	Y	
*inter*Media	Y	Y	
Oracle Text	Y	Y	
Additional Database Features			
Database event triggers	Y	Y	
DBMS_REPAIR package	Y	Y	
DBMS_METADATA package	Y	Y	
Drop column	Y	Y	
Rename column, constraint	Y	Y	
Index-organized table	Y	Y	
Instead-of triggers	Y	Y	
LOB (large object) support	Y	Y	
Locally-managed tablespaces	Y	Y	
LogMiner	Y	Y	
Multiple block size support	Y	Y	
Plan stability	Y	Y	
Reverse key index	Y	Y	
Temporary table	Y	Y	

Oracle reserves the right to make changes to the contents of this paper at a later date.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 221
3698
Doc.

8402
A.

ORACLE

Oracle9i Database Product Family
June 2003
Author: Sandra Cheevers
Contributing Authors: Jenny Tsai

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Oracle Corporation provides the software
that powers the internet.

Oracle is a registered trademark of Oracle Corporation. Various product and service names referenced herein may be trademarks of Oracle Corporation. All other product and service names mentioned may be trademarks of their respective owners.

Copyright © 2001 Oracle Corporation
All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 222
3698
Doc.

8404
A.

Summary management	N	Y	
Long operations monitor	Y	Y	
Direct Path Load API	Y	Y	
Export transportable tablespace	N	Y	
Import transportable tablespace	Y	Y	
External tables	Y	Y	
MERGE	Y	Y	
Multi-table insert	Y	Y	
Pipelined table functions	Y	Y	
Synchronous Change Data Capture	N	Y	
Integration			
Oracle Streams	N	Y	
Advanced Queuing	Y	Y	
Oracle Workflow	Y	Y	
Messaging Gateway to IBM MQSeries	N	Y	
Basic Replication	Y	Y	Updatable materialized view site
Advanced Replication	N	Y	Multi-master replication
Distributed queries	Y	Y	
Distributed transactions	Y	Y	
Heterogeneous Services	Y	Y	
Networking			
Connection pooling	Y	Y	
Oracle Connection Manager	N	Y	
Oracle Names	Y	Y	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 223
Doc. 3698

8406
A.

Microsoft Transaction Server/COM+ integration	Y	Y	Windows only
Oracle OLE DB Provider	Y	Y	Windows only
Oracle Objects for OLE (OO4O)	Y	Y	Windows only
VLM Support	Y	Y	Windows only
OLE DB.NET and ODBC.NET support	Y	Y	Windows only
Native .NET Data Provider – ODP.NET	Y	Y	Windows only
64-bit Itanium support for Windows, Linux, and HP-UX	Y	Y	
Globalization support	Y	Y	
Autonomous transactions	Y	Y	
SQL*Plus	Y	Y	
iSQL*Plus	Y	Y	
Manageability			
Oracle Enterprise Manager	Y	Y	
Oracle Change Management Pack	N	Y	Extra cost option
Oracle Diagnostics Pack	N	Y	Extra cost option
Oracle Tuning Pack	N	Y	Extra cost option
Oracle Management Pack for SAP R/3	N	Y	Extra cost option
Automatic undo management	Y	Y	
Self-tuning memory management	Y	Y	
Server managed backup and recovery	Y	Y	
Recovery Manager	Y	Y	
Legato Storage Manager	Y	Y	
Duplexed backup sets	N	Y	

DOS 06/2005 - CN
CPMI - CORREIOS
Fls. Nº 224
3698
Doc.

8408
A.

FEATURE AND PRODUCT AVAILABILITY

Not all features and options are available with all editions of the Oracle9*i* Database Release 2.

Oracle9*i* Personal Edition is available on Windows2000, Windows NT, Windows XP and Windows Server 2003 (32-bit and 64-bit). It includes at no extra cost all features and options that are available with Oracle9*i* Enterprise Edition, such as Oracle Partitioning and Oracle Advanced Security, with the exception of the Oracle Real Application Clusters option.

See the following table for Oracle9*i* Database Standard Edition and Oracle9*i* Database Enterprise Edition feature and option availability.

High Availability			
Oracle Data Guard – Redo Apply	N	Y	
Oracle Data Guard – SQL Apply	N	Y	
Basic readable standby database	Y	Y	
Fast-start selectable recovery time	N	Y	
Online index build	N	Y	
Online table reorganization/redefinition	N	Y	
Online index coalesce	N	Y	
Global index maintenance during DDL	Y	Y	
Flashback Query	Y	Y	
Quiesce database	N	Y	
Block-level media recovery	N	Y	
Incremental backup and recovery	N	Y	
Online backup and recovery	Y	Y	
Parallel backup and recovery	N	Y	
Point-in-time tablespace recovery	N	Y	
Trial recovery	N	Y	
Oracle Fail Safe	Y	Y	Windows only

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 225
Doc: 3698

8410
A

view of the data. Range, hash, composite (range combined with hash), and list partitioning methods are supported.

Oracle Advanced Security

Oracle Advanced Security is an Oracle9*i* Enterprise Edition option that provides strong authentication and encryption by implementing industry standard encryption and integrity algorithms as well as supporting several external authentication services. The product provides robust Enterprise User Security where organizations have a choice of implementing end-to-end security by authenticating users using digital certificates or passwords, reducing the total cost of deploying security.

Oracle Label Security

Oracle Label Security provides sophisticated and flexible security based on row labels for fine-grained access control. Oracle Label Security employs labeling concepts used by government, defense and commercial organizations to protect sensitive information and provide data separation and includes a powerful tool to manage policies, labels, and user label authorizations.

Oracle OLAP

Fully integrated in the database, Oracle OLAP provides a complete set of analytical functions. Predictive analysis can be used to forecast market trends, predict product manufacturing requirements, and build enterprise budgeting and financial analysis systems, for example. Using complex, multidimensional queries and calculations, information such as market shares and net present value can be derived. The Java OLAP API provides efficient object-orientation for building applications that require complex analytical queries.

Oracle Data Mining

Oracle Data Mining allows companies to build advanced business intelligence applications that mine corporate databases, discover new insights, and integrate that information into business applications. Oracle Data Mining embeds data mining functionality for making classifications, predictions, and associations. All model-building and scoring functions are accessible through a Java-based API.

Oracle Spatial

Oracle Spatial allows users and application developers to seamlessly integrate their spatial data into enterprise applications. Oracle Spatial facilitates analysis based on the spatial relationships of associated data, like the proximity of store locations to customers within a given distance and sales revenue per territory. Oracle Spatial manages spatial data in an industry-standard database, resulting in application integration that takes place at the data server. This enables

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 226
Doc. 3698

8412
A.

Oracle9*i* Database Release 2 Product Family

INTRODUCTION

Oracle9*i* Database Release 2 is available in three editions, each suitable for different development and deployment scenarios. Oracle also offers several additional optional database products that enhance the capabilities of Oracle9*i* Database for specific application requirements. The following are the three available editions of Oracle9*i* Database Release 2:

- Oracle9*i* Database Standard Edition delivers unprecedented ease-of-use, power, and price/performance for workgroup, department-level, and internet/intranet applications. Oracle9*i* Database Standard Edition includes a fully integrated set of easy-to-use management tools, full distributed, replication, and web features. From single-server environments for small businesses to highly distributed branch environments, Oracle9*i* Database Standard Edition includes all the facilities necessary to build business-critical applications. Oracle9*i* Database Standard Edition can only be licensed on servers that have a maximum capacity of 4 processors.
- Oracle9*i* Database Enterprise Edition provides efficient, reliable, secure data management for high-end applications such as high volume on-line transaction processing (OLTP) environments, query-intensive data warehouses, and demanding Internet applications. Oracle9*i* Database Enterprise Edition provides the tools and functionality to meet the availability and scalability requirements of today's mission-critical applications for the enterprise.
- Oracle9*i* Database Personal Edition supports single user development and deployment that require full compatibility with Oracle9*i* Standard Edition and Oracle9*i* Enterprise Edition. By bringing the award-winning functionality of Oracle9*i* Database to the personal workstation, Oracle offers a database that combines the power of the world's most popular database with the ease of use and simplicity you would expect in a desktop product.

Oracle9*i* Personal Edition, Oracle9*i* Standard Edition and Oracle9*i* Enterprise Edition include a common set of application development features including SQL object-relational capabilities and PL/SQL and Java programmatic interfaces for writing stored procedures and triggers. Applications written for

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 227
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 228
3698
Doc.

8403
A.

Oracle9*i*

Release Notes

Release 2 (9.2.0.1.0) for HP 9000 Series HP-UX (64-bit)

June 2002

Part No. A97350-02

This document accompanies Oracle9*i* release 2 (9.2.0.1.0) for HP 9000 Series HP-UX (64-bit). Its contents supplement or supersede information in the installation guide for this release, or in the Oracle9*i* documentation library.

Topics:

- System Requirements
- Documentation
- Installation Issues
- Product-Related Issues
- Post-Installation Issues
- Known Bugs

System Requirements

Except as noted here, system requirements are in the installation guide for this release, and are current as of the release date.

Hard Disk Space Requirements

The space requirements listed on the Available Products window apply to installations that include a database. If you select the Software Only configuration type, then you will require 3 GB.

Additional Software Patch Requirements

If you are installing Oracle Real Application Clusters on HP-UX 11.0, and if you are using the HMP protocol, then you must download the following patch from HP in addition to the patches listed in the installation guide.

ORACLE

Copyright © 2002, Oracle Corporation
All rights reserved.

Oracle is a registered trademark, and Oracle7, Oracle8*i*, Oracle9*i*, Oracle*MetaLink*, Oracle Names, Oracle Transparent Gateway, PL/SQL, Pro*C, Pro*COBOL, Pro*FORTRAN and SQL*Plus are trademarks or registered trademarks of Oracle Corporation. Other names may be trademarks of their respective owners.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 229
3698
Doc.

8399
A.

Oracle Universal Installer Version Update

Oracle9*i* release 2 (9.2.0.1.0), which is provided with the release, uses Oracle Universal Installer 2.2.0.12.0. This version number supersedes the version listed in the installation guide.

Documentation

Additional product `README` files are located in their respective product directories under the `$ORACLE_HOME` directory and in the `$ORACLE_HOME/relnotes` directory.

Documentation Errata

The following is a list of errors in the documentation for this release.

PL/SQL Gateway

In Appendix A, "Oracle9*i* Components," in *Oracle9i Installation Guide Release 2 (9.2.0.1.0) for UNIX Systems*, PL/SQL Gateway is listed as a supported product. It has been desupported for this release.

Pre-Installation Requirements

Under "Random Access Memory" on page 2-3 in Chapter 2, "Pre-Installation Requirements, in *Oracle9i Installation Guide Release 2 (9.2.0.1.0) for UNIX Systems*, the Linux and HP commands are reversed. The correct commands are the following:

Linux

```
$ grep MemTotal /proc/meminfo
```

HP

```
$ /usr/sbin/dmesg | grep "Physical:"
```

Installation Issues

This section provides information about the following topics:

- 32-bit O/S Support
- Multiple CD-ROM Installation
- runInstaller Script
- Installing Databases with Database Configuration Assistant
- Database Migration

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 230
Doc. 3698

- Installing with Response Files

32-bit O/S Support

Do not run Oracle9*i* on a 32-bit operating system. Oracle9*i* release 2 (9.2.0.1.0) is offered in a 64-bit version only. If you try to run any 64-bit executables on a 32-bit operating system, then they will fail. If you run Oracle9*i* release 2 (9.2.0.1.0) on a 32-bit system, then you will see the following error message:

```
./oracle: Exec format error. Wrong Architecture.
```

Multiple CD-ROM Installation

During the installation of Oracle9*i* release 2 (9.2.0.1.0), you will be prompted to insert additional CD-ROMs from the set that make up Oracle9*i* release 2 (9.2.0.1.0). When prompted to mount the next CD-ROM, use the following procedure:

1. On the window where you have started the Installer, press Enter to go to the UNIX prompt, and then change the directory to your system's root directory. Log in as the `root` user by using the following commands:

   ```
   $ cd /
   $ su root
   ```

2. Unmount and remove the CD-ROM from the CD-ROM drive with the following command:

   ```
   # /usr/sbin/pfs_umount/SD_CDROM
   ```

3. Insert the required CD-ROM into the CD-ROM drive and mount it by using the following command:

   ```
   # /usr/sbin/pfs_mount/SD_CDROM
   ```

4. Click OK to continue.

runInstaller Script

Because it is necessary to insert and eject more than one CD-ROM during installation, you must not launch Oracle Universal Installer by running the `runInstaller` script from a shell where the current working directory is the CD-ROM mount point, or by clicking on the script in the *File Manager* window. In an X Window environment, it is possible to launch the Installer this way, but then the installation will fail because you will not be able to eject a software CD-ROM until you end the installation session.

8391
A.

Installing Databases with Database Configuration Assistant

Review the following information before running Database Configuration Assistant.

SYS and SYSTEM Password Change Requirement

If you use Database Configuration Assistant to create a database, be aware that you will be required to change the SYS and SYSTEM passwords at the end of the configuration process. This is a new security procedure designed to protect access to your data.

Database Migration

If you are upgrading from release 8.0.6 to release 9.2.0.1.0 and you have Oracle *inter*Media installed on your system, then you cannot use Database Migration Assistant. You must migrate the database manually. For information on manual database migration, refer to *Oracle9i Database Migration Release 2 (9.2).*

Installing with Response Files

For installation with a response file, the path to the response file must be the full path on the system. The Oracle Universal Installer does not handle relative paths properly.

Unzip Utility for Downloading and Installing Oracle Patches

An unzip utility is provided with Oracle9*i* release 2 (9.2.0.1.0) for uncompressing Oracle patches downloaded from Oracle*MetaLink*. The utility is located in the following directory:

```
$ORACLE_HOME/bin/
```

Product-Related Issues

This section provides information on the following topics:

- Character Sets
- Demo Schema
- Java Database Connectivity Driver
- Oracle Advanced Security
- Oracle Internet Directory (OID)
- Oracle Real Application Clusters

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 231
3698
Doc.

Character Sets

The following section provides information on restrictions and updates to character sets.

Oracle9*i* NCHAR Datatypes

In Oracle9*i* release 2 (9.2.0.1.0), the SQL NCHAR datatypes are limited to the Unicode character set encoding (UTF8 and AL16UTF16). Alternative character sets such as the fixed-width Asian character set JA16SJISFIXED in Oracle8*i* are no longer supported.

To migrate existing NCHAR, NVARCHAR, and NCLOB columns, export and import NCHAR columns, complete the following steps:

1. Export all SQL NCHAR columns from Oracle8*i*.
2. Drop the SQL NCHAR columns.
3. Migrate the database to Oracle9*i*.
4. Import the SQL NCHAR columns in to Oracle9*i*.

AL24UTFFSS Character Set

Oracle9*i* release 2 (9.2.0.1.0) does not support the Unicode character set AL24UTFFSS introduced in Oracle7. This character set was based on the Unicode standard 1.1, which is now obsolete.

Oracle9*i* release 2 (9.2.0.1.0) supports the Unicode database character sets AL32UTF8 and UTF8. These database character sets include the Unicode enhancements based on the Unicode standard 3.0.

To migrate the existing AL24UTFFSS database, upgrade your database character set to UTF8 before upgrading to Oracle9*i*. Oracle Corporation recommends that you use the Character Set Scanner for data analysis before attempting to migrate your existing database character set.

Character Set Scanner

Set the LD_LIBRARY_PATH variable to include the `$ORACLE_HOME/lib` directory before running the Character Set Scanner (csscan) from the `$ORACLE_HOME` directory. If you do not correctly set the LD_LIBRARY_PATH variable, then the csscan utility will fail.

Demo Schema

If you select a multibyte character set or UTF as the national character set in Oracle9*i* release 2 (9.2.0.1.0), then you must recreate the demo schema and the database installation.

8395
A.

For more information on creating schemas, schema dependencies and requirements, refer to the `readme.txt` file in the `$ORACLE_HOME/demo/schema` directory.

Java Database Connectivity Driver

The default behavior for the `ResultSet::getXXXStream()` has been modified to comply with the Java Database Connectivity (JDBC) specification so that the APIs return null values for database null `LONG/LONG RAW` values.

For Oracle8*i* release 8.1.*x* JDBC drivers, the default behavior was to return an empty stream for database null values. The Java property `jdbc.backward_compatible_to_8.1.7` allows the system to use the earlier JDBC default behavior when using the Oracle9*i* drivers and applies to Oracle9*i* JDBC Thin and OCI drivers.

For example, if the Java property is set at the virtual machine runtime, the following command will cause the Oracle9*i* JDBC drivers to return empty streams from calls to `ResultSet::getXXXStream()`:

```
java -Djdbc.backward_compatible_to_8.1.7 myJavaProgram
```

Oracle Advanced Security

If you install `jsse.jar` and `jcert.jar` as extensions (located in `$JAVA_HOME/jre/lib/ext`), then you must also install `jssl-1_1.jar` in the same directory.

Oracle Internet Directory (OID)

Review the following information if you intend to install Oracle Internet Directory (OID).

Starting Up OID Server

By default, the OID server is started on port 389. If this port is unavailable, then OID server is started on a different port, which is logged in the following file:

`$ORACLE_HOME/ldap/install/oidca.out`

Custom Installation and Global Database Name

When performing a custom Oracle Internet Directory installation, do not change the global database name or the Oracle SID.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 232
Doc. 3698

Upgrade from Enterprise Edition Oracle9*i* or Oracle8*i*

If you have installed in the same ORACLE_HOME either Oracle Internet Directory release 3.0.1.*x* and the complete release of Oracle9*i* (9.0.1) Enterprise Edition, or Oracle Internet Directory 2.1.1.*x* and the complete release of Oracle8*i* (8.1.7) Enterprise Edition, then you must first upgrade Oracle Internet Directory to the release 9.2.0.*x*.*x* version, and then upgrade as a separate step either Oracle9*i* Enterprise Edition Release 1 (9.0.1) or Oracle8*i* release 3 (8.1.7) to Oracle9*i* Enterprise Edition Release 2 (9.2.0.*x*.*x*).

> **See Also:** *Oracle Internet Directory README* for more information on Oracle Internet Directory utilities, and necessary pre-upgrade and post-upgrade tasks.

Oracle Real Application Clusters

Review the following section if you will install Oracle Real Application Clusters.

Restrictions for Installing Real Application Clusters

The following restrictions apply for this release:

- The Cluster Manager implementation may not be able to handle 32-bit and 64-bit clients concurrently. This will prevent 32-bit and 64-bit Oracle Real Application Clusters executables from being used at the same time within the same cluster domain.

  If a database is not set up with the Oracle Real Application Clusters option, then this restriction does not apply to the Oracle executables.

- If you are installing Oracle9*i* release 2 (9.2.0.1.0) Real Applications Clusters on a cluster that already contains an ORACLE_HOME for a previous release of Real Application Clusters, then you must run the Oracle Universal Installer from the cluster node with the oraInventory installation registry. Doing this ensures that product installation inventories are synchronized on the nodes with information about existing ORACLE_HOME directories.

Real Application Clusters Custom Installation Requirement

If you plan to create an Oracle Enterprise Manager repository in an existing database, and you plan to use the DRSYS tablespace for the repository, then ensure that the DRSYS tablespace raw device data file has an additional 50 MB of free space. This is in addition to the 250 MB size documented for this raw device.

8393
A.

Real Application Clusters and Database Upgrade Assistant

If you use Database Upgrade Assistant to upgrade an earlier Oracle database version (the "source" database) to Oracle9*i* release 2 (9.2.0.1.0) (the "target" database), then the upgraded database will always use the server parameter file SPFILE by default to store `init.ora` file parameters. If the source database also uses SPFILE (either a cluster filesystem file or a shared raw device), then the upgraded target database also uses the same SPFILE.

If the source database does not use an SPFILE, then the target database uses a default server parameter file, `spfile.ora`, which is located in the `$ORACLE_HOME/dbs/` directory.

If your platform does not support a cluster file system, then you must move the SPFILE to a shared raw device, using the following procedure:

1. Create an SPFILE with the following commands:

```
$ sqlplus "/ as sysdba"
SQL> create pfile='?/dbs/initdbname.ora' from
spfile='?/dbs/spfile.ora';
SQL> create spfile='/dev/oracle_vg/dbname_spfile' from
pfile='?/dbs/initdbname.ora';
SQL> exit;
```

   where *dbname* is the name of your cluster database.

2. Go to the `$ORACLE_HOME/dbs` directory using the following command:

```
$ cd $ORACLE_HOME/dbs
```

3. Create an `$ORACLE_HOME/dbs/initsid.ora` file, where *sid* is the system identifier of the instance on the node. The `initsid.ora` file must contain the following line:

```
SPFILE='/dev/oracle_vg/dbname_spfile'
```

4. Copy the `initsid.ora` file to the remote nodes on which the cluster database has an instance with the following commands:

```
$ rcp initsid.ora nodex:$ORACLE_HOME/dbs/initsidx.ora
```

   where *sidx* is the system identifier of the instance on node *x*. Repeat the preceding `rcp` command for each member node of the cluster database.

5. Restart the cluster database with the following command syntax:

```
$ srvctl stop database -d dbname
$ srvctl start database -d dbname
```

EROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 203
3698
Doc.

Real Application Clusters and Database Configuration Assistant

The following section provides information on using Database Configuration Assistant (DBCA) to create a Real Application Clusters database.

Placing Datafiles On a Shared Non-OFA Cluster Configuration

If your ORACLE_HOME directory is not on a shared cluster filesystem partition, but you want to place datafiles, controlfiles, redo log files, or other database files on a shared cluster filesystem partition, then invoke DBCA using the following syntax to create the cluster database:

```
$ dbca -datafileDestination pathname
```

where *pathname* is the location where you want files to be placed.

For example, to place datafiles in the path `/ora/oradata`, give the following command:

```
$ dbca -datafileDestination /ora/oradata
```

Note: For optimal performance and data security, Oracle Corporation recommends that you configure your database in accordance with the Optimal Flexible Architecture (OFA) standard. For more information on OFA, refer to *Oracle9i Administrator's Reference for UNIX Systems*.

Real Application Clusters Instance Management

After you have created a cluster database using DBCA, SYSDBA privileges are revoked for all users. As SYSDBA, you must grant SYSDBA privileges explicitly to the database user account that you plan to use for adding or deleting an instance to or from the cluster database.

For example, to grant SYSDBA privileges to the administrative user SYS, issue the following commands:

```
$ sqlplus "/ as sysdba"
SQL> grant sysdba to sys;
SQL> exit;
```

Oracle Real Application Clusters and Upgrading from Oracle8*i*

If you are upgrading from Oracle8*i*, then set the `instance_number` initialization parameter in the `init.ora` file for all instances.

8391
A.

Oracle Real Application Clusters and HyperMessaging Protocol (HMP)

Complete the following three tasks prior to using HMP:

Ensure HF Software is Installed and Verified Ensure that you have the HyperFabric software installed, and verify that it exists. The HF software product ID number is B6257AA. Verify that it exists with the following command:

```
swlist | grep -i B6257AA
```

Configure HyperFabric Patch Use the following command to verify that the HyperFabric patch is configured properly before installing Oracle9*i*:

```
/opt/clic/bin/clic_stat
```

If the HyperFabric patch is configured properly, then the response to this command will list all nodes in the cluster. If cluster members are missing, then they will not appear in the response.

Note: The Hyper Messaging Protocol is not supported on V-class HP systems.

Tune HMP parameters Oracle Corporation recommends that you review parameters and tune them according to HP guidelines for optimal HMP performance. A list of HMP-tunable parameters can be found in the following file:

```
/opt/clic/lib/skgxp/skclic.conf
```

To enable Oracle to use HMP and to relink the Oracle binary with HMP, complete the following steps:

1. Set up your environment on all nodes
2. Shut down the database
3. Enter the following commands on all nodes:

```
$ cd $ORACLE_HOME/rdbms/ub
$ make -F ins_rdbms.mk ipc_hms ioracle
```

Platform-Specific Product Information

The following product information in this section supersedes the information in the installation guide for Oracle9*i* release 2 (9.2.0.1.0) on HP-UX.

- Precompiler Options:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc. 3698

- Pro*COBOL (32-bit and 64-bit) are supported.
- Pro*FORTRAN (32-bit and 64-bit) are supported.
- SQL Module for Ada is not supported.

- Oracle Advanced Security:
  - Radius challenge response authentication is not supported.
  - CyberSafe is not supported.
  - DCE Integration is not supported.
- JDBC/OCI Interfaces:
  - Oracle JDBC Thin Driver for JDK 1.4 is not supported.
  - Oracle JDBC/OCI Driver for JDK 1.4 is not supported.

Post-Installation Issues

This section presents issues that can occur during post-installation:

Control File Size Limits

In addition to the database, a number of other Oracle features use control files to record metadata. The maximum size of control files is limited by the size of the minimum data block size that your operating system permits. On HP-UX, the minimum data block size is 2048 bytes, and the maximum size of control files is 20000 database blocks.

Support for 32-bit Client Applications

Oracle9*i* (64-bit) provides support for both 32-bit clients as well as 64-bit clients. By default, all demos and clients provided with this release link and run in 64-bit mode. You can, however, build 32-bit and 64-bit clients in the same `$ORACLE_HOME`.

The following combinations will run and link successfully in Oracle9*i* (64-bit):

- 32-bit applications against a 64-bit Oracle Server
- 64-bit applications against a 64-bit Oracle Server

The 64-bit client shared library is:

```
$ORACLE_HOME/lib/libclntsh.sl
```

The 32-bit client shared library is:

```
$ORACLE_HOME/lib32/libclntsh.sl
```

8389
A.

Building 32-bit Pro*C Customer Applications

Both 32-bit and 64-bit customer applications are supported in this release. Refer to the following files for further information:

```
$ORACLE_HOME/precomp/demo/demo_proc.mk
$ORACLE_HOME/precomp/demo/demo_proc32.mk
```

Building 32-bit OCI Customer Applications

Both 32-bit and 64-bit Oracle Call Interface (OCI) customer applications are supported in this release. Refer to the following file for further information:

```
$ORACLE_HOME/rdbms/demo/demo_rdbms.mk
```

32-bit Files and Directories

In Oracle9*i* (64-bit) for HP-UX (64-bit), the following directories contain 32-bit executables and libraries:

- `$ORACLE_HOME/lib32`
- `$ORACLE_HOME/rdbms/lib32`
- `$ORACLE_HOME/hs/lib32`
- `$ORACLE_HOME/network/lib32`
- `$ORACLE_HOME/precomp/lib32`

How to Determine Whether Segments or Tablespaces are Using Compression

The following section provides additional information about database management.

Segments and Compression Settings

To find out which database segments are using compression, log in to the database as the user SYS, and create the view `all_segs` with the following create or replace view statement:

```
SQL> create or replace view all_segs
       (owner, segment_name,
         partition_name, spare1
as
select u.name, o.name, o.subname, s.spare1
from sys.user$ u, sys.obj$ o, sys.ts$ ts, sys.sys_objects so,
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 235
3698
Doc.

```
     sys.seg$ s, sys.file$ f
where s.file# = so.header_file
   and s.block# = so.header_block
   and s.ts# = so.ts_number
   and s.ts# = ts.ts#
   and s.ts# = so.object_id
   and o.owner# = u.user#
   and s.type# = so.object_type_id
   and s.ts# = f.ts#
   and s.file# = f.relfile#
union all
select u.name, un.name, NULLL, NULL
from sys.user$ u, sys.ts$ ts, sys.undo $ un, sys.seg$ s,
     sys.file$ f
where s.file# = un.file#
   and s.block# = un.block
   and s.ts# = un.ts#
   and s.ts# = ts.ts#
   and s.user# = u.user#
   and s.type# in (1, 10)
   and un.status$ != 1
   and un.ts# = f.ts#
   and un.file# = f.relfile#
union all
select u.name, to_char(f.file#)|| '.' || to_char(s.block#), NULL, NULL
from sys.user$ u, sys.ts$ ts, sys.seg$ s, sys.file$ f
where s.ts# = ts.ts#
   and s.user# = u.user#
   and s.type# not in (1, 5, 6, 8, 10)
   and s.ts# = f.ts#
   and s.file# = f.relfile#
/
```

After creating this view, you can issue queries against the view to find out whether a segment currently is compressed, as illustrated in the following examples:

- To determine if a segment is currently compressed, apply the following predicate in a query to the column `spare1`:

  ```
  bitand(spare1, 2048) > 0
  ```

  For example, to see if segments currently are compressed, issue a statement similar to the following:

  ```
  SQL> select * from all_segs where bitand(spare1,2048) > 0;
  ```

- To determine if a segment contains any compressed blocks, apply the following predicate in a query:

  ```
  bitand(spare1, 4096) > 0
  ```

8337
A-

For example, to see which segments contain any compressed blocks, issue a statement similar to the following:

```
SQL> select * from all_segs where bitand(spare1, 4096) > 0;
```

Tablespaces and Compression Settings

When you want to determine compression settings on a table space, log in as SYS, and create the view `compression_ts` with the following create or replace view statement:

```
SQL> create or replace view compression_ts (tablespace_name, flags) as
select ts.name, ts.flags from
sys.ts$ ts where ts.online$ !=3;
```

After creating this view, you can issue queries against it to find out the compression state of tablespaces, such as determining if a tablespace is currently set as DEFAULT COMPRESS, or DEFAULT NOCOMPRESS, as illustrated in the following examples:

- To determine if a tablespace is currently set as DEFAULT COMPRESS, use the following predicate:

  ```
  bitand(flags, 64) > 0
  ```

  For example, to see which tablespaces are currently DEFAULT COMPRESS, issue a statement similar to the following:

  ```
  SQL> select * from compression_ts where bitand(flags, 64) > 0
  ```

- To determine if a tablespace is currently set as DEFAULT NOCOMPRESS, use the following predicate:

  ```
  bitand(flags, 64) == 0
  ```

  For example, to see which tablespaces are currently DEFAULT NOCOMPRESS, issue a statement similar to the following:

  ```
  select * from compression_ts where bitand(flags, 64) == 0;
  ```

Known Bugs

The following is a list of known bugs that affect Oracle9*i* release 2 (9.2.0.1.0):

Error in JSP/Servlet Script

There is a path error in the `$ORACLE_HOME/bin/ojspc script`. This path error causes the script to fail. To correct this error:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 236
Doc. 3698

1. Open the script
2. Find `$ORACLE_HOME/jsp/lib/servlet.jar`
3. Correct it to read `$ORACLE_HOME/lib/servlet.jar`
4. Save the script

Error Installing OLAP CWMLITE Tablespace

During installation, if you select Online Analytic Processing (OLAP) services, perform multiple installations on the same system, and create new databases during these installations, then CWMLite may have an invalid OLAP CWMLITE tablespace registry. Oracle Corporation has assigned bug identification number 2359208 to track this problem.

To work around this problem, use the following procedure after you have completed installation:

1. Ensure that the database and the listener are running.
2. Using the following command, start SQL*Plus as the administrative user SYS:

   ```
   sqlplus "/ as sysdba"
   ```

3. Using the following command, enable the display of text within the PL/SQL block:

   ```
   SQL> set serveroutput on;
   ```

4. Using the following command, verify whether the OLAP CWMLITE tablespace is valid:

   ```
   SQL> execute
   dbms_output.put_line(sys.dbms_registry.is_valid('AMD'));
   ```

   If the preceding command returns `0`, then the OLAP CWMLITE tablespace is invalid. Go to step 5.

   If the preceding command returns `1`, then the OLAP CWMLITE tablespace is valid, and no further testing needs to be done.

5. If the OLAP CWMLITE tablespace is invalid, turn on echoing with the following command:

   ```
   SQL> execute cwm2_olap_manager.Set_Echo_on;
   ```

6. Validate the OLAP CMWLITE tablespace with the following command:

   ```
   SQL> execute cwm2_olap_installer.Validate_CWM2_Install;
   ```

- PHNE_26551

If you are installing Oracle Real Application Clusters on HP-UX version 11*i* (11.11), and if you are using the HMP protocol, then you must download the following patch from HP in addition to the patches listed in the installation guide.

- PHNE_27114

If you are installing HP-UX version 11*i* (11.11), then you must download the following OS patches:

- GOLDQPK11i (includes both GOLDAPPS11i and GOLDBASE11i)
- PHKL_25506
- PHSS_26263
- PHSS_24638
- JDK 1.3.1.02

If you are using ServiceGuard OPS Edition version 11.13 for HP-UX lli, then you must install the following patch:

- PHSS_26674

> **Note:** In the near future, *ServiceGuard OPS Edition* will be replaced with *ServiceGuard Extension for RAC*.

Updated Requirements

Oracle Corporation updates these release notes online at the following site:

`http://docs.oracle.com`

If you need assistance with navigating the Oracle documentation site, refer to the following site:

`http://docs.oracle.com/instructions.html`

Refer also to the Certify Web Pages on Oracle*MetaLink*, which provide certified configuration information for Oracle and non-Oracle products. To access Certify:

1. Register or log in to Oracle*MetaLink* at the following Web address:

   `http://metalink.oracle.com`

2. Select Product Lifecycle from the Oracle*Metalink* navigation bar.
3. Select Certifications in the Product Lifecycle window navigation bar.

8385
A.

After entering the preceding command, the OLAP CWMLITE registry is validated. During this process, screen messages list database objects such as Dimension, Dimension Attribute, and Level, and where these objects are created.

7. When the output stops, enter the following command to verify that the OLAP CWMLITE registry is now valid:

```
SQL> execute
dbms_output.put_line(sys.dbms_registry.is_valid('AMD'));
```

If the preceding command returns `0`, then the OLAP CWMLITE registry is still invalid. Review your installation logs for other errors.

If the preceding command returns 1, then the OLAP CWMLITE tablespace is valid, and no further testing needs to be done.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 237
Doc. 3698

Apêndice HN

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 2268
Doc. 3698

8383
A-

JD Edwards' OneWorld Xe Implementation and Certification With Hewlett-Packard's MC/ServiceGuard High Availability Software

JD Edwards Home Page

The HP Partner Technology Center (PTAC) has successfully integrated OneWorld Xe with MC/ServiceGuard. The implementation and certification of OneWorld Xe followed the PTAC's High Availability Implementation and Certification Process.

Information regarding this process, and how other ISVs may take advantage of this service, is available in these PTAC documents:

Appendix 33: HP's Partner Technology Access Center High Availability Implementation and Certification Services Datasheet

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

PARTNER TECHNOLOGY ACCESS CENTER
nº 03/2005 - CN
CORREIOS
Fls Nº 239
Doc. 3698

8382 A

Executive Overview

JD Edwards and OneWorld Xe

With approximately 5,700 customers and 5,000 employees — as well as $944 million in revenue in fiscal year 1999 — J.D. Edwards (NASDAQ: JDEC) is the leading supplier of e-business solutions that deliver speed and agility for customers throughout the world. For more than 20 years, J.D. Edwards has provided innovative, flexible solutions essential to running complex and fast-moving multinational organizations — acting as a true business partner to help companies of all sizes leverage existing investments, take advantage of new technologies, and maintain competitive advantage.

What most distinguishes J.D. Edwards is its customer-centric Idea to Action™ value proposition, an industry-redefining approach to collaborative business software solutions. Idea to Action helps you use information technology efficiently throughout the virtual enterprise, easily tailoring applications to meet changing business needs. It gives you the freedom to put your ideas into action quickly in a B2B world.

OneWorld® Xe, the company's new "extended enterprise" product, boasts some 300 Internet-ready applications that enable companies to choose the most appropriate collaborative solutions to meet their business needs.

OneWorld Xe, with capabilities enhanced via J.D. Edwards' eXtended Process Integration (XPI) engine, will allow customers to use open, flexible and interoperable technologies that foster communication and commerce among suppliers and customers across their extended supply chain.

With OneWorld Xe's key defined areas of functionality — ranging from customer relationship management to integrated supply chain and fulfillment management — J.D. Edwards customers can optimize a factory, a distribution channel or an entire supply chain network.

"We have already seen tremendous customer demand for OneWorld Xe," said Glenn Tubb, senior vice president of development of J.D. Edwards. "Giving our customers open collaboration is empowering them to automate and streamline business processes across the supply chain to increase shareholder value and optimize working capital."

Currently, J.D. Edwards has over 1,000 customers that are live on various releases of OneWorld as well as dozens of OneWorld Xe customers who have been using the product in beta form. Beta customers on OneWorld Xe include Praxair, a $4.7 billion global pioneer in the industrial gases industry; Ontario Store Fixtures, the leading North American manufacturer of complete retail store interiors; Grupo LaLa, a Mexican holding company in the food industry; Fisher & Paykel Industries Ltd., a New Zealand-based manufacturer of home appliances and healthcare items; and Cascade Designs, a manufacturer of outdoor, travel, and wheel chair cushion products.

Richest Functionality

J.D. Edwards' OneWorld Xe combines the best of back office software, enterprise applications integration (EAI) and inter-enterprise process workflow into one solution, with new features that achieve the following benefits:

- Lasting Value. OneWorld's event-driven, component-based architecture is enhanced to increase reach and agility. OneWorld Xe automatically generates intuitive Windows, HTML and Java user interfaces from one set of business specifications, allowing users to choose their interface of choice. Its configurable, Web-based portal serves as the single point of entry into OneWorld and can be tailored to meet the access and collaboration needs of partners, suppliers and customers. With intuitive change management capabilities, OneWorld Xe allows users to make changes to existing processes, activate additional capabilities or manage upgrades.
- Collaboration based on standards-based interoperability. OneWorld Xe supports XML-based business-to-business interoperability technology from Netfish, and enterprise application technology from Active Software (a.k.a. WebMethods). J.D. Edwards is embedding these technologies into its eXtended

Process Integration engine, OneWorld XPI, which will serve as the integration platform or "broker" that addresses both internal enterprise application portfolios and external interoperability with customers' and trading partners' business systems.

- Freedom to Choose pre-integrated e-business applications. With OneWorld Xe, J.D. Edwards tightens integration with strategic partner solutions and delivers notable new and enhanced functionality, including:
- Enhanced advanced planning, providing best-in-class collaboration, real-time order promising, and new functionality for discrete industries.
- An intelligent, role- and relationship-based messaging which will support real-time collaboration among multiple trading community partners.
- Web-enabled demand planning module for collaboration on forecasts and improved geographical mapping capabilities to more accurately represent facility locations.
- New storefront options with Microsoft Commerce Server and IBM WebSphere Commerce Suite, which are pre-integrated with OneWorld Xe.
- Knowledge management solution (slated for availability in early 2001) for gathering data from document repositories, Intranets, data warehouses, supply chains and the Internet and delivering it to employees, partners and customers for integrated decision support. Using data warehouse development tools, any database can be used as a business intelligence source. New and updated information is automatically pushed to users' desktop, phone, fax, wireless device or OneWorld portal.
- Application integrations to deliver extended solutions, including Siebel eConsumer Goods in J.D. Edwards Solutions for Consumer Industries; Extensity time, travel and expense management; and Ariba Buyer.
- Self-service options to increase productivity and improve response with secure, self-service portals that automate most routine query-and-update tasks. Managers can initiate personnel actions; suppliers can respond to quotes, initiate date change requests, inquire on orders, receipts, inventory levels and payment information; and carriers can inquire on assigned loads and shipments.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 240
3698
Doc.

8380
E-

High Availability with HP MC/ServiceGuard

HP Multi-Computer/ServiceGuard (MC/ServiceGuard) is a specialized facility for protecting mission-critical applications from a wide variety of hardware and software failures. With MC/ServiceGuard, multiple— up to 16—nodes (systems) are organized into an enterprise cluster that delivers highly available application services to LAN-attached clients.

HP MC/ServiceGuard monitors the health of each node and quickly responds to failures in a way that minimizes or eliminates application downtime. MC/ServiceGuard is able to automatically detect and respond to failures in the following components:

- System processors
- System memory
- LAN media and adapters
- System processes
- Application processes

Application Packages
With HP MC/ServiceGuard, application services and all the resources needed to support the application are bundled into special entities called application packages. These application packages are the basic units that are managed and moved within an enterprise cluster. Packages simplify the creation and management of highly available services and provide outstanding levels of flexibility for workload balancing.

Fast Detection of Failure, Fast Restoration of Applications
Within an enterprise cluster, HP MC/ServiceGuard monitors hardware and software components, detects failures, and responds by promptly allocating new resources to support mission-critical applications. The process of detecting the failure and restoring the application service is completely automated—no operator intervention is needed.

Recovery times provided by HP MC/ServiceGuard for LAN adapter failures are extremely fast, typically within a few seconds. Recovery times for failures requiring the switch of an application to an alternate node will vary, depending on the software services being used by the application. For example, a database application that is using a logging facility would need to perform transaction rollbacks as part of the recovery process. The time needed to perform this transaction rollback would be part of the total time to recover the application. MC/ServiceGuard will detect the node failure, reconfigure the cluster, and begin executing the startup script for the application package on an alternate node in less than 30 seconds.

High Availability for Mission-Critical Applications

99.95% Uptime Commitment—The Mission-Critical Server Suites (MCSS) is HP's platform solution, offering an unprecedented 99.95% uptime commitment. Pre-configured and tested, MCSS is based on MC/ServiceGuard-enabled HP 9000 Enterprise Servers, packaged with the consulting and support services necessary to ensure success in your mission-critical environment.

MCSS solutions are available on HP 9000 R-, L-, N-, K-, and V-Class servers; and high availability storage is offered on either disk arrays with AutoRAID, or the HP SureStore E XP256 or XP512, providing the ultimate in data availability, reliability, and high performance.

Other Benefits of MC/ServiceGuard:
-Availability during Hardware and Software Maintenance
-Online Reconfiguration Reduces Planned Downtime
-Workload Balancing
-Protecting Data Integrity

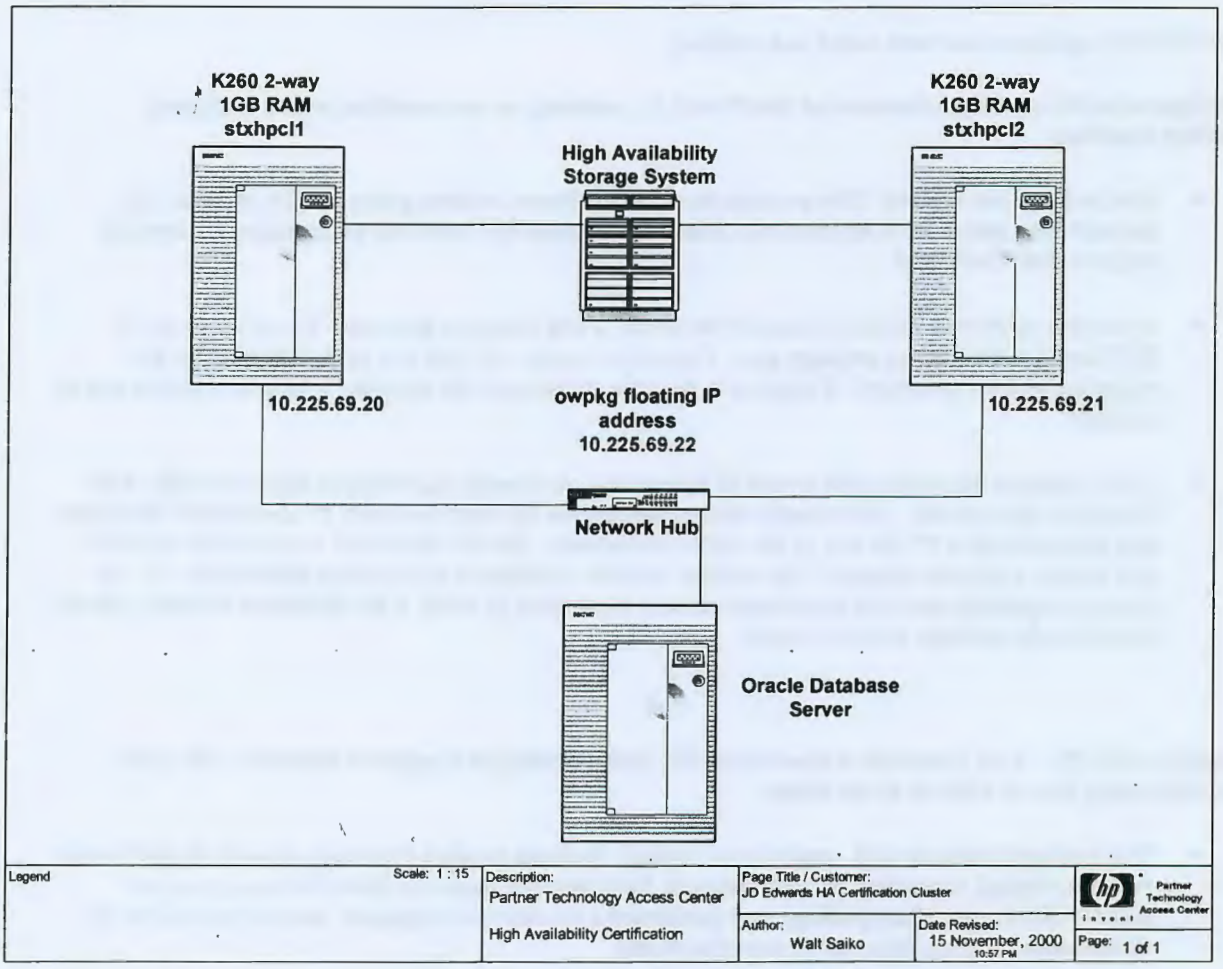
For more information, contact any of our worldwide sales offices or HP Channel Partners (in the U.S. call 1-800-637-7740).

8379
A.

OneWorld Xe in a Highly-Available Environment

Integrating OneWorld Xe with MC/ServiceGuard provides redundancy and high availability for OneWorld Xe. This integration provides:

- minimal downtime in the event of a system failure
- automatic response to the user interface that owns running OneWorld batch jobs
- minimal delay before running OneWorld batch jobs are able to be restarted
- no reconfiguration of clients in a client/server environment; the ServiceGuard movement of the OneWorld server to another physical node is transparent to the client nodes.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 241
Doc. 3698

In the first configuration tested, one primary node was used (stxhpcl1), with a second node initially not performing any OneWorld-related activity (stxhpcl2) (standby node). Both the active and standby nodes were connected to a High Availability Storage System (HASS) disk storage mechanism via FWD SCSI connection. The HASS contained the MC/ServiceGuard cluster lock disk, shared OneWorld Xe files and instance information needed by both the primary OneWorld node and the standby OneWorld node (upon a failover).

An additional node was part of this configuration. This node was configured as an Oracle Database Server. The Oracle Database has been previously certified as compatible with MC/ServiceGuard; thus, for this certification effort, it was decided that only OneWorld Xe would be configured in a failover architecture.

A remote node was connected via TCP/IP LAN to the same subnet as stxhpcl1 and stxhpcl2. This remote node, running Windows NT, was used to run the OneWorld Xe client software. This node was the source of client/server requests to the OneWorld Xe server, and was also used to submit batch jobs to the OneWorld Xe server.

Two different configurations were tested and certified:

Configuration #1 – A Single Instance of OneWorld Xe, running on one machine, with a dedicated standby machine.

- One package was created. This package mounted the shared volume group and file systems. The package then performed a set user (su) command, invoked the OneWorld environment, and ran the script to start OneWorld.

- A monitor script was written to monitor the jdenet_n and jdequeue processes. The script is run by MC/ServiceGuard during package start. The monitor script will stay in a loop, checking for the existence of these processes. If either or both of these processes do not exist, a failover scenario will be initiated.

- A HA Monitor was configured as part of the package, to monitor the available filesystem size of the OneWorld filesystems. This monitor was maintained by MC/ServiceGuard. If the available filesystem size dropped below 5% for any of the shared filesystems, MC/ServiceGuard would report this error, and initiate a failover scenario. This monitor was also configured as a package dependency, i.e. the package depended upon this filesystem resource to perform its work. If the filesystem resource was not available, the package would not start.

Configuration #2 – Two Instances of OneWorld Xe, each running on a separate machine, with each machine being able to failover to the other.

- Two packages were created, owpkg1 and owpkg2. Package owpkg1 is primary on node stxhpcl1 while package owpkg2 is primary on node stxhpcl2. Each package mounts a shared volume group and separate file system. Each package then performed a set user (su) command, invoked the OneWorld environment, and ran the script to start OneWorld.

- Once both packages had been started by MC/ServiceGuard, two separate and operational instances of OneWorld Xe were running. Each instance had its own IP address, own volume group and own file system. In actual operation, one OneWorld instance could have been used for interactive operation, while the other instance could have been used for batch operations.

- Each instance of OneWorld Xe accessed a common database owned by the Oracle Database Server, which was described earlier within this document.

invent 8377 A.

- A monitor script was written to monitor the jdenet_n and jdequeue processes. The script is run by MC/ServiceGuard during package start. The monitor script will stay in a loop, checking for the existence of these processes. If either or both of these processes do not exist, a failover scenario for that package will be initiated.

- A HA Monitor was configured as part of the package, to monitor the available filesystem size of the OneWorld filesystems. This monitor was maintained by MC/ServiceGuard. If the available filesystem size on either machine dropped below 5% for any of the shared filesystems, MC/ServiceGuard would report this error, and initiate a failover scenario for that package. This monitor was also configured as a package dependency, i.e. the package depended upon this filesystem resource to perform its work. If the filesystem resource was not available, the package would not start.

The OneWorld Xe application is validated and certified by Hewlett-Packard as compatible with Hewlett-Packard's MC/ServiceGuard high availability software. OneWorld Xe can be monitored by MC/ServiceGuard, with the level of monitoring highly configurable and subject to the implementation plans of the customer.

This document details a set of tests showing that OneWorld Xe is compatible with MC/ServiceGuard. The tests show that if a node running a OneWorld Xe batch job fails, the job can be restarted on an alternate node in less than 30 seconds. Also, any client-server connections to failed OneWorld Xe processes can be reconnected to the OneWorld server running on an alternate node.

MC/ServiceGuard packages are dependent on having automated application startup and shutdown scripts. HP engineers have developed package configuration and control scripts that are suitable for use (after system-specific modification) in a OneWorld Xe production environment.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 242
3691
Doc.

8376 A-

OneWorld Xe Implementation and Certification in an MC/ServiceGuard Cluster

The process followed for the certification of OneWorld Xe in an MC/ServiceGuard environment is detailed in:

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

Implementation and Certification Onsite Process Participants:

Hewlett-Packard: Walt Saiko (Partner Technology Access Center)
JD Edwards: Roger Miller (Server Technology)

invent 8375 A.

MC/ServiceGuard Configuration

Configuration 1 – Single Instance of OneWorld Xe

Configuring the Cluster

Create the ASCII cluster template file

```
cmquerycl –v –C /etc/cmcluster/cluster1.ascii –n stxhpcl1 –n stxhpcl2
```

Modify the template (cluster1.ascii) to reflect the environment and to verify the cluster configuration.

```
cmcheckconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Create the cluster by applying the configuration file. This will create the binary file "cmclconfig" and automatically distribute it among the nodes defined in the cluster.

```
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Start the cluster and check the cluster status. Test the cluster halt also.

```
cmruncl –v –n stxhpcl1 –n stxhpcl2
cmviewcl –v
cmhaltcl –f –v
cmruncl –n stxhpcl1 –n stxhpcl2
```

Configuring a ServiceGuard Package on the Primary Node.

Create the package configuration files and tailor to the test environment. Do not include the second node at this stage.

```
cd /etc/cmcluster
mkdir owpkg
cmmakepkg –p owpkg.ascii          # Edit owpkg.ascii
```

Create package control scripts and tailor to the test environment. Do not include application startup/shutdown, service monitoring, or relocatable IP address at this stage.

```
cd owpkg
cmmakepkg –s control.sh
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
```

Test cluster and package startup. Unmount all logical volumes on shared volume group and deactivate the volume group

```
cmruncl                           # Start cluster and package
cmviewcl –v                       # Check that package has started
```

Add knowledge of the Secondary Node to the packages

```
edit owpkg.ascii
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
```

Test cluster and package startup.. Unmount all logical volumes on shared volume group and deactivate the volume group

```
cmruncl                           # Start cluster and package
cmviewcl –v                       # Check that package has started
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 243
3698
Doc.

374
A.

Assign the dynamic IP address of the package.

```
Edit control.sh file to include dynamic IP address
cmhaltpkg owpkg
cmrunpkg –v owpkg
cmviewcl –v                          # Check package has started and dynamic IP
                                     # address is pingable
```

Enable the OneWorld Xe application to switch to a second node by editing the package control file

```
edit owpkg.ascii                     # add NODE_NAME stxhpcl2
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
cmhaltcl –f –v
cmruncl –v
```

Test package switching to stxhpcl2

```
cmhaltpkg owpkg                      # Halt package

cmmodpkg –e owpkg                    # Enable package switching

cmrunpkg -n stxhpcl2 owpkg
```

Add in OneWorld Xe startup/shutdown details to package control script (control.sh) and check successful package activation.

```
Edit control.sh file to include Oneworld Xe startup/shutdown
cmrunpkg –v owpkg
cmviewcl –v                          # Check package has started on node stxhpcl1
                                     # and OneWorld Xe binary is running
```

Test package switching to stxhpcl2

```
cmhaltpkg owpkg                      # Activate owpkg on stxhpcl2
cmmodpkg –e owpkg                    # verify OneWorld Xe binary running
cmrunpkg –n stxhpcl2 owpkg           # Enable package switching
```

invent
8373
A.

Configuration 2 – Multiple Instances of OneWorld Xe

Configuring the Cluster

Create the ASCII cluster template file

```
cmquerycl –v –C /etc/cmcluster/cmclconfig.ascii –n stxhpcl1 –n stxhpcl2
```

Modify the template (cluster1.ascii) to reflect the environment and to verify the cluster configuration.

```
cmcheckconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Create the cluster by applying the configuration file. This will create the binary file "cmclconfig" and automatically distribute it among the nodes defined in the cluster.

```
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Start the cluster and check the cluster status. Test the cluster halt also.

```
cmruncl –v –n stxhpcl1 –n stxhpcl2
cmviewcl –v
cmhaltcl –f –v
cmruncl –n stxhpcl1 –n stxhpcl2
```

Configuring a ServiceGuard Package on Each Node.

Create the package configuration files and tailor to the test environment. Do not include the second node at this stage.

```
cd /etc/cmcluster
mkdir owpkg1
cmmakepkg –p owpkg.ascii        # Edit owpkg1.ascii
mkdir owpkg2
cmmakepkg -p owpkg2.ascii       # Edit owpkg2.ascii
```

Create package control scripts and tailor to the test environment. Do not include application startup/shutdown, service monitoring, or relocatable IP address at this stage.

```
cd owpkg1
cmmakepkg –s control.sh

cd ../owpkg2
cmmakepkg –s control.sh
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg1.ascii -P owpkg2.ascii
```

Test cluster and package startup. Unmount all logical volumes on shared volume group and deactivate the volume groups

```
cmruncl                         # Start cluster and packages
cmviewcl –v                     # Check that packages have started
```

Add knowledge of the appropriate Secondary Node to the packages

```
edit owpkg1.ascii
edit owpkg2.ascii
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg1.ascii -P owpkg2.ascii
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 244
Doc. 3698

8312
A.

Test cluster and package startup.. Unmount all logical volumes on shared volume groups and deactivate the volume groups

```
cmruncl                                  # Start cluster and packages
cmviewcl –v                              # Check that packages have started
```

Assign the dynamic IP addresses of the packages.

Edit both control.sh files to include dynamic IP addresses

```
cmrunpkg –v owpkg1
cmrunpkg –v owpkg2
cmviewcl –v                              # Check packages have started and dynamic IP
                                         # addresses are pingable
```

Enable the OneWorld Xe application to switch to a second node by editing the package control files

```
edit owpkg1.ascii                        # add NODE_NAME stxhpcl2
edit owpkg2.ascii                        # add NODE_NAME stxhpcl1
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg1.ascii -P owpkg2.ascii
cmhaltcl –f –v
cmruncl –v
```

Test package switching to the alternate node

```
cmhaltpkg owpkg1                         # Halt packages
cmhaltpkg owpkg2

cmmodpkg –e owpkg1                       # Enable package switching
cmmodpkg -e owpkg2

cmrunpkg -n stxhpcl2 owpkg1
cmrunpkg -n stxhpcl1 owpkg2
```

Add in OneWorld Xe startup/shutdown details to package control scripts (control.sh) and check successful package activation.

Edit control.sh files to include OneWorld Xe startup/shutdown

```
cmrunpkg –v owpkg1
cmrunpkg –v owpkg2
cmviewcl –v                              # Check packages have started and OneWorld
                                         # binaries are running
```

Test package switching to the alternate node

```
cmhaltpkg owpkg1                         # Activate owpkg1 & owpkg2
cmhaltpkg owpkg2                         # verify OW binaries running
cmmodpkg –e owpkg1                       # Enable package switching
cmmodpkg -e owpkg2
cmrunpkg -n stxhpcl2 owpkg1
cmrunpkg -n stxhpcl1 owpkg2
```

Test Suite

Output of cmviewcl –v with the two servers, stxhpcl1 and stxhpcl2, up and running. This is the multiple instance configuration.

```
CLUSTER       STATUS
hpcluster     up

  NODE          STATUS       STATE
  stxhpcl1      up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH          NAME
    PRIMARY       up           10/12/6       lan0

    PACKAGE       STATUS       STATE         PKG_SWITCH    NODE
    owpkg1        up           running       enabled       stxhpcl1

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM        STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service     up                 0          0   owmonitor
      Subnet      up                                10.225.69.0
      Resource    up                                /system/filesystem/availMb/tmp

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING     NAME
      Primary       up           enabled       stxhpcl1      (current)
      Alternate     up           enabled       stxhpcl2

  NODE          STATUS       STATE
  stxhpcl2      up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH          NAME
    PRIMARY       up           10/12/6       lan0

    PACKAGE       STATUS       STATE         PKG_SWITCH    NODE
    owpkg2        up           running       enabled       stxhpcl2

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM        STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service     up                 0          0   owmonitor2
      Subnet      up                                10.225.69.0

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING     NAME
      Primary       up           enabled       stxhpcl2      (current)
      Alternate     up           enabled       stxhpcl1
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 245
Doc. 3698

8370
A

Failover Test Scenarios

Test 1
Test package shutdown script execution.

Begin by bringing the packages UP on their Primary node. Use <ps -ef | grep jdenet> to verify that OW is up and running, and that the package IP addresses are pingable.

<cmhaltpkg> the OW packages. Check to confirm that the OW binaries are not running.

Test 2
Test package startup.

This test should be performed immediately following Test 1. With the OW packages down on their Primary nodes, start the packages using ServiceGuard command <cmrunpkg>, specifying that the packages should start on their Primary node.

Verify using <ps> that the OW processes are running. Interact with the processes using the client interface, and verify the results of the operation that is requested.

Test 3
Test local failure of LAN card in Primary machine to verify that the OW packages being tested use the standby LAN interface card when the Primary LAN interface card has failed.

Begin with the OW packages running on their Primary nodes. Disconnect each primary data LAN cable from designated ports on the network hub.

After a delay of several seconds, the LAN switch should occur. Verify that the OW packages (owpkg1 and owpkg2) are still pingable via their dynamic IP addresses, using the original Package IP addresses on the Standby Data LAN interface card.

Test 4
Restore LAN connectivity disconnected in Test 3, and confirm that switch back to the primary LAN occurs.

Begin by verifying that the OW packages are running on the Primary node.

After reconnecting the LAN cable of LAN0 to the hub, LAN contact to the package should hang for 1-2 seconds, until ServiceGuard has performed the LAN switch. After this time, confirm that LAN0 (Primary Data LAN) is now active once again.

Test 5
Test Powerfail switchover.

Begin with the OW packages running on their Primary nodes. Power off ONE of the Primary nodes by disconnecting the power cord from that node.

Verify the ServiceGuard package switch process occurs. The ServiceGuard Cluster Manager daemon should automatically recognize the loss of the Primary node heartbeat. The cluster reforms with the other healthy member, including the Secondary node for owpkg1 package. The cluster should free leftover holds on shared volume group(s) and the owpkg1 application should restart on the Secondary node.

Verify that the owpkg1 package is accessible via the client interface.

Note: when the Primary node is restarted, it will automatically rejoin the cluster, but it will not be enabled for package switching. No package switchback should occur at this time.

8369

Test 6

Test the failover capability of a ServiceGuard-monitored OW application. In the owpkg1 package control script, monitor.sh is a service run by ServiceGuard It has a restart setting of 0. Confirm that when the monitor process is killed, a failover is initiated.

Begin with the OW packages being tested running on their primary nodes, under normal operating conditions.

Kill the monitor.sh process. Verify that ServiceGuard recognizes the loss of the monitored service, and initiates a failover.

Confirm that the OW package starts correctly on its Secondary node and that the OW binaries are running.

Test 7

Test the monitoring and exiting capability of the monitor.sh monitor process. Confirm that the monitor script is correctly monitoring all specified processes, and that failure of one of the monitored processes is reported. Failure of a monitored processed is reported by the monitor script returning an exit code of 1. This will initiate a ServiceGuard failover.

Begin with the OW packages operating under normal conditions on their primary nodes.

Find a monitored process using <ps -ef | grep jdenet> Terminate the process using the <kill -9 pid> command.

This will cause monitor.sh to return an exit code 1 to ServiceGuard. ServiceGuard will recognize that the service has exited with an error code, and perform a package halt on that node. ServiceGuard will then initiate a package failover to the Secondary node.

Confirm that the OW package starts correctly on the Secondary node, and that the OW package is accessible via the client interface.

Test 8

Test OW performance when the cluster heartbeat is totally lost.

For both the Primary and Secondary nodes for the packages, disconnect both primary and standby cluster heartbeat cables from the network hub. Altogether, four cables have been disconnected.

One and only one of the nodes should take control of the cluster lock disk and win the quorum.

If the Primary node takes control of the cluster lock disk: the owpkg1 package will continue running normally on the Primary node. The Secondary node will perform a TOC in order to avoid a potential race condition, and to remove locks held on the shared volume group used by owpkg2. The Primary node will take control of the shared volume group used by the owpkg2 package and start the owpkg2 package as if a normal failover had taken place. Package switching for both packages will be disabled since there is no other cluster member that can be contacted via network heartbeat

If the Secondary node takes control of the cluster lock disk: the owpkg2 package will continue running normally on the Secondary node. The Primary node will perform a TOC in order to avoid a potential race condition, and to remove locks held on the shared volume group used by owpkg1. The Secondary node will take control of the shared volume group used by the owpkg1 package and start the owpkg1 package as if a normal failover had taken place. Package switching for both packages will be disabled since there is no other cluster member who can be contacted via network heartbeat.

Through either path above, the OW packages should now be running on one of the cluster member.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 246
Doc. 3698

8368 A

Test 9

Test package failover when both the primary and standby LAN fail.

With the owpkg1 package running on its Primary node under normal conditions and under a typical workload, disconnect the Primary and Standby LAN on the Primary node.

Verify that the ServiceGuard Cluster Manager daemon recognizes loss of the data path. The cluster should reform with one healthy member, the Secondary node The primary node should free leftover holds on shared volume group(s). The owpkg1 package should start up correctly on its Secondary node.

Note: When the Primary node is reconnected, it will automatically rejoins the cluster, but is not enabled for package switching. No package switchback will occur at this time.

Appendix 1: OneWorld Xe cluster configuration file (cmclconfig.ascii)

```
# **********************************************************************
# ********* HIGH AVAILABILITY CLUSTER CONFIGURATION FILE ***************
# ***** For complete details about cluster parameters and how to    ****
# ***** set them, consult the cmquerycl(1m) manpage or your manual. ****
# **********************************************************************

# Enter a name for this cluster.  This name will be used to identify the
# cluster when viewing or manipulating it.

CLUSTER_NAME            hpcluster


# Cluster Lock Device Parameters.  This is the volume group that
# holds the cluster lock which is used to break a cluster formation
# tie.  This volume group should not be used by any other cluster
# as cluster lock device.

FIRST_CLUSTER_LOCK_VG         /dev/vgcl1


# Definition of nodes in the cluster.
# Repeat node definitions as necessary for additional nodes.

NODE_NAME               stxhpcl1
  NETWORK_INTERFACE     lan0
    HEARTBEAT_IP                10.225.69.20
  FIRST_CLUSTER_LOCK_PV         /dev/dsk/c0t1d0
# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE    /dev/tty0p0

# Primary Network Interfaces on Bridged Net 1: lan0.
#   Warning: There are no standby network interfaces on bridged net 1.

NODE_NAME               stxhpcl2
  NETWORK_INTERFACE     lan0
    HEARTBEAT_IP                10.225.69.21
  FIRST_CLUSTER_LOCK_PV         /dev/dsk/c1t1d0
# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE    /dev/tty0p0

# Primary Network Interfaces on Bridged Net 1: lan0.
#   Warning: There are no standby network interfaces on bridged net 1.


# Cluster Timing Parmeters (microseconds).

HEARTBEAT_INTERVAL              1000000
NODE_TIMEOUT            2000000


# Configuration/Reconfiguration Timing Parameters (microseconds).

AUTO_START_TIMEOUT      600000000
NETWORK_POLLING_INTERVAL        2000000

# Package Configuration Parameters.
# Enter the maximum number of packages which will be configured in the cluster.
# You can not add packages beyond this limit.
# This parameter is required.
MAX_CONFIGURED_PACKAGES         9


# List of cluster aware Volume Groups. These volume groups will
# be used by package applications via the vgchange -a e command.
```


invent
8367
A.
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 247
Doc. 3698

8366 A.

```
# For example:
# VOLUME_GROUP          /dev/vgdatabase.
# VOLUME_GROUP          /dev/vg02.

VOLUME_GROUP            /dev/vgcl1
VOLUME_GROUP            /dev/vgcl2
```

Appendix 2: OneWorld Xe owpkg1 package configuration file (owpkg1.ascii)

8365
A.

```
# **********************************************************************
# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE (template) *******
# **********************************************************************
# ******* Note: This file MUST be edited before it can be used. ********
# * For complete details about package parameters and how to set them, *
# * consult the MC/ServiceGuard or ServiceGuard OPS Edition manpages   *
# * or manuals.                                                        *
# **********************************************************************

# Enter a name for this package.  This name will be used to identify the
# package when viewing or manipulating it.  It must be different from
# the other configured package names.

PACKAGE_NAME                    owpkg1


# Enter the failover policy for this package. This policy will be used
# to select an adoptive node whenever the package needs to be started.
# The default policy unless otherwise specified is CONFIGURED_NODE.
# This policy will select nodes in priority order from the list of
# NODE_NAME entries specified below.
#
# The alternative policy is MIN_PACKAGE_NODE. This policy will select
# the node, from the list of NODE_NAME entries below, which is
# running the least number of packages at the time this package needs
# to start.

FAILOVER_POLICY                         CONFIGURED_NODE


# Enter the failback policy for this package. This policy will be used
# to determine what action to take when a package is not running on
# its primary node and its primary node is capable of running the
# package. The default policy unless otherwise specified is MANUAL.
# The MANUAL policy means no attempt will be made to move the package
# back to its primary node when it is running on an adoptive node.
#
# The alternative policy is AUTOMATIC. This policy will attempt to
# move the package back to its primary node whenever the primary node
# is capable of running the package.

FAILBACK_POLICY                 -       MANUAL


# Enter the names of the nodes configured for this package.  Repeat
# this line as necessary for additional adoptive nodes.
# Order IS relevant.  Put the second Adoptive Node AFTER the first
# one.
# Example : NODE_NAME  original_node
#           NODE_NAME  adoptive_node

NODE_NAME                       stxhpc11
NODE_NAME                       stxhpc12


# Enter the complete path for the run and halt scripts.  In most cases
# the run script and halt script specified here will be the same script,
# the package control script generated by the cmmakepkg command.  This
# control script handles the run(ning) and halt(ing) of the package.
# If the script has not completed by the specified timeout value,
# it will be terminated.  The default for each script timeout is
# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full
# execution of each script.
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT                      /etc/cmcluster/owpkg1/control.sh
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 218
3698
Doc.

8364

```
RUN_SCRIPT_TIMEOUT              NO_TIMEOUT
HALT_SCRIPT                     /etc/cmcluster/owpkg1/control.sh
HALT_SCRIPT_TIMEOUT             NO_TIMEOUT

# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names.  All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
# specified SERVICE_HALT_TIMEOUT, the cluster software will send
# out the SIGKILL signal to the service to force its termination.
# This timeout value should be large enough to allow all cleanup
# processes associated with the service to complete.  If the
# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be
# assumed, meaning the cluster software will not wait at all
# before sending the SIGKILL signal to halt the service.
#
# Example: SERVICE_NAME                   DB_SERVICE
#          SERVICE_FAIL_FAST_ENABLED      NO
#          SERVICE_HALT_TIMEOUT           300
#
# To configure a service, uncomment the following lines and
# fill in the values for all of the keywords.
#
#SERVICE_NAME                   <service name>
#SERVICE_FAIL_FAST_ENABLED      <YES/NO>
#SERVICE_HALT_TIMEOUT           <number of seconds>

SERVICE_NAME                    owmonitor
SERVICE_FAIL_FAST_ENABLED       NO
SERVICE_HALT_TIMEOUT   100


# Enter the network subnet name that is to be monitored for this package.
# Repeat this line as necessary for additional subnet names.  If any of
# the subnets defined goes down, the package will be switched to another
# node that is configured for this package and has all the defined subnets
# available.

SUBNET                  10.225.69.0


# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,
# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify Package
# Resource Dependencies.  To define a package Resource Dependency, a
# RESOURCE_NAME line with a fully qualified resource path name, and
# one or more RESOURCE_UP_VALUE lines are required.  The
# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are optional.
#
# The RESOURCE_POLLING_INTERVAL indicates how often, in seconds, the
# resource is to be monitored.  It will be defaulted to 60 seconds if
# RESOURCE_POLLING_INTERVAL is not specified.
#
# The RESOURCE_START option can be set to either AUTOMATIC or DEFERRED.
# The default setting for RESOURCE_START is AUTOMATIC.  If AUTOMATIC
# is specified, ServiceGuard will start up resource monitoring for
```

invent

8363
A.

```
# these AUTOMATIC resources automatically when the node starts up.
# If DEFERRED is selected, ServiceGuard will not attempt to start
# resource monitoring for these resources during node start up.  User
# should specify all the DEFERRED resources in the package run script
# so that these DEFERRED resources will be started up from the package
# run script during package run time.
#
# RESOURCE_UP_VALUE requires an operator and a value.  This defines
# the resource 'UP' condition.  The operators are =, !=, >, <, >=,
# and <=, depending on the type of value.  Values can be string or
# numeric.  If the type is string, then only = and != are valid
# operators.  If the string contains whitespace, it must be enclosed
# in quotes.  String values are case sensitive.  For example,
#
#                                   Resource is up when its value is
#                                   --------------------------------
#       RESOURCE_UP_VALUE      = UP                    "UP"
#       RESOURCE_UP_VALUE      != DOWN                 Any value except "DOWN"
#       RESOURCE_UP_VALUE      = "On Course"           "On Course"
#
# If the type is numeric, then it can specify a threshold, or a range to
# define a resource up condition.  If it is a threshold, then any operator
# may be used.  If a range is to be specified, then only > or >= may be used
# for the first operator, and only < or <= may be used for the second operator.
# For example,
#                                   Resource is up when its value is
#                                   --------------------------------
#       RESOURCE_UP_VALUE      = 5             5                       (threshold)
#       RESOURCE_UP_VALUE      > 5.1           greater than 5.1        (threshold)
#       RESOURCE_UP_VALUE      > -5 and < 10   between -5 and 10       (range)
#
# Note that "and" is required between the lower limit and upper limit
# when specifying a range.  The upper limit must be greater than the lower
# limit.  If RESOURCE_UP_VALUE is repeated within a RESOURCE_NAME block, then
# they are inclusively OR'd together.  Package Resource Dependencies may be
# defined by repeating the entire RESOURCE_NAME block.
#
# Example : RESOURCE_NAME               /net/interfaces/lan/status/lan0
#           RESOURCE_POLLING_INTERVAL 120
#           RESOURCE_START            AUTOMATIC
#           RESOURCE_UP_VALUE         = RUNNING
#           RESOURCE_UP_VALUE         = ONLINE
#
#           Means that the value of resource /net/interfaces/lan/status/lan0
#           will be checked every 120 seconds, and is considered to
#           be 'up' when its value is "RUNNING" or "ONLINE".
#
# Uncomment the following lines to specify Package Resource Dependencies.
#
#RESOURCE_NAME             <Full_path_name>
#RESOURCE_POLLING_INTERVAL  <numeric_seconds>
#RESOURCE_START             <AUTOMATIC/DEFERRED>
#RESOURCE_UP_VALUE         <op> <string_or_numeric> [and <op> <numeric>]
RESOURCE_NAME                /system/filesystem/availMb/tmp
RESOURCE_POLLING_INTERVAL           60
RESOURCE_START              AUTOMATIC
RESOURCE_UP_VALUE >         50


# The default for PKG_SWITCHING_ENABLED is YES. In the event of a
# failure, this permits the cluster software to transfer the package
# to an adoptive node.  Adjust as necessary.

PKG_SWITCHING_ENABLED         YES


# The default for NET_SWITCHING_ENABLED is YES.  In the event of a
# failure, this permits the cluster software to switch LANs locally
# (transfer to a standby LAN card).  Adjust as necessary.

NET_SWITCHING_ENABLED         YES
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 249
Doc. 3698

```
# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,
# in the event of a failure, the cluster software will halt the node
# on which the package is running.  Adjust as necessary.

NODE_FAIL_FAST_ENABLED NO
```

invent

8361
A.

Appendix 3: OneWorld Xe owpkg1 package control script (control.sh)

```
#"(#) A.11.09                                          $Date: 08/06/1999 $".
# ************************************************************************
# *                                                                      *
# *        HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)           *
# *                                                                      *
# *                                                                      *
# ************************************************************************

# UNCOMMENT the variables as you set them.

# Set PATH to reference the appropriate directories.
PATH=/usr/bin:/usr/sbin:/etc:/bin

# VOLUME GROUP ACTIVATION:
# Specify the method of activation for volume groups.
# Leave the default ("VGCHANGE="vgchange -a e") if you want volume
# groups activated in exclusive mode. This assumes the volume groups have
# been initialized with 'vgchange -c y' at the time of creation.
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and comment
# out the default, if your disks are mirrored on separate physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"), and comment
# out the default, if your disks are mirrored on separate physical paths,
# and you want the mirror resynchronization to ocurr in parallel with
# the package startup.
#
# Uncomment the third line (VGCHANGE="vgchange -a y") if you wish to
# use non-exclusive activation mode. Single node cluster configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a e -q n -s"
# VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"              # Default

# VOLUME GROUPS
# Specify which volume groups are used by this package. Uncomment VG[0]=""
# and fill in the name of your first volume group. You must begin with
# VG[0], and increment the list in sequence.
#
# For example, if this package uses your volume groups vg01 and vg02, enter:
#         VG[0]=vg01
#         VG[1]=vg02
#
# The volume group activation method is defined above. The filesystems
# associated with these volume groups are specified below.
#
VG[0]=/dev/vgcl1

# FILESYSTEMS
# Specify the filesystems which are used by this package. Uncomment
# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name of your first
# logical volume, filesystem and mount option for the file system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with read and
# write options enter:
#          LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a; FS_MOUNT_OPT[0]="-o rw"
#          LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b; FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying the logical
# volume, the mount point and the mount options for the file system. Each
# filesystem will be fsck'd prior to being mounted. The filesystems will be
# mounted in the order specified during package startup and will be unmounted
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 250
Doc. 3698

8360

```
# in reverse order during package shutdown. Ensure that volume groups
# referenced by the logical volume definitions below are included in
# volume group definitions above.
#
LV[0]=/dev/vgcl1/lv01; FS[0]=/u03; FS_MOUNT_OPT[0]=""

# FILESYSTEM UNMOUNT COUNT
# Specify the number of unmount attempts for each filesystem during package
# shutdown.  The default is set to 1.
FS_UMOUNT_COUNT=1

# IP ADDRESSES
# Specify the IP and Subnet address pairs which are used by this package.
# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of your first
# IP and subnet address. You must begin with IP[0] and SUBNET[0] and
# increment the list in sequence.
#
# For example, if this package uses an IP of 192.10.25.12 and a subnet of
# 192.10.25.0 enter:
#          IP[0]=192.10.25.12
#          SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)
#
# Hint: Run "netstat -i" to see the available subnets in the Network field.
#
# IP/Subnet address pairs for each IP address you want to add to a subnet
# interface card.  Must be set in pairs, even for IP addresses on the same
# subnet.
#
IP[0]=10.225.69.22
SUBNET[0]=10.225.69.0

# SERVICE NAMES AND COMMANDS.
# Specify the service name, command, and restart parameters which are
# used by this package. Uncomment SERVICE_NAME[0]="", SERVICE_CMD[0]="",
# SERVICE_RESTART[0]="" and fill in the name of the first service, command,
# and restart parameters. You must begin with SERVICE_NAME[0], SERVICE_CMD[0],
# and SERVICE_RESTART[0] and increment the list in sequence.
#
# For example:
#          SERVICE_NAME[0]=pkg1a
#          SERVICE_CMD[0]="/usr/bin/X11/xclock -display 192.10.25.54:0"
#          SERVICE_RESTART[0]=""  # Will not restart the service.
#
#          SERVICE_NAME[1]=pkg1b
#          SERVICE_CMD[1]="/usr/bin/X11/xload -display 192.10.25.54:0"
#          SERVICE_RESTART[1]="-r 2"   # Will restart the service twice.
#
#          SERVICE_NAME[2]=pkg1c
#          SERVICE_CMD[2]="/usr/sbin/ping"
#          SERVICE_RESTART[2]="-R" # Will restart the service an infinite
#                                  number of times.
#
# Note: No environmental variables will be passed to the command, this
# includes the PATH variable. Absolute path names are required for the
# service command definition.  Default shell is /usr/bin/sh.
#
SERVICE_NAME[0]=owmonitor
SERVICE_CMD[0]="/etc/cmcluster/owpkg1/monitor.sh"
SERVICE_RESTART[0]="-r 0"
#SERVICE_CMD[0]=""
#SERVICE_RESTART[0]=""

# DEFERRED_RESOURCE NAME
# Specify the full path name of the 'DEFERRED' resources configured for
# this package.  Uncomment DEFERRED_RESOURCE_NAME[0]="" and fill in the
# full path name of the resource.
#
#DEFERRED_RESOURCE_NAME[0]=""

# DTC manager information for each DTC.
# Example: DTC[0]=dtc_20
```

invent
8359
A.

```
#DTC_NAME[0]=


# START OF CUSTOMER DEFINED FUNCTIONS

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# started.  You can create as many functions as you need.

function customer_defined_run_cmds
{
# ADD customer defined run commands.
: # do nothing instruction, because a function must contain some command.

       su oneworld <<EOF1
        . /u03/oneworld/b733_sp14/system/bin32/owenv
        /u03/oneworld/b733_sp14/system/bin32/RunOneWorld.sh
EOF1

       test_return 51
}

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# halted.

function customer_defined_halt_cmds
{
# ADD customer defined halt commands.
: # do nothing instruction, because a function must contain some command.
      su oneworld <<EOF2
        . /u03/oneworld/b733_sp14/system/bin32/owenv
        /u03/oneworld/b733_sp14/system/bin32/EndOneWorld.sh now
EOF2
       test_return 52
}

# END OF CUSTOMER DEFINED FUNCTIONS


# START OF RUN FUNCTIONS


function activate_volume_group
{
for I in ${VG[@]}
do
       if [[ "${VGCHANGE}" = "vgchange -a y" ]]
       then
              print "$(date '+%b %e %X') - Node \"$(hostname)\": Activating volume group $I
with non-exclusive option."
       else
              print "$(date '+%b %e %X') - \"$(hostname)\": Activating volume group $I with
exclusive option."
       fi

       $VGCHANGE $I
       test_return 1

       # If the -s option has been specified, then we perform
       # the resynchronization as a background task
       #
       if [[ ${VGCHANGE#*-s} != ${VGCHANGE} ]]
       then
           {
              if /sbin/vgsync $I
              then
                  print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronized volume
group $I"
              else
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 251
3698
Doc.

```
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronization of
volume group $I encountered an error"
            fi
        } &
    fi
done
}

# For each {file system/logical volume} pair, fsck the file system
# and mount it.  If the file system is busy, mounting of the file
# system will fail, the control script will exit with an error.

function check_and_mount
{
integer R=0

for I in ${LV[@]}
do
    if [[ $(mount -p | awk '$1 == "'$I'"') = "" ]]
    then
        RLV[$R]="${I%/*}/r${I##*/}"

        if [ -x /usr/sbin/fstyp ]
        then
                fstype[$R]=$(fstyp $I)
        fi
        (( R = $R + 1 ))
    fi
done

# Verify that there is at least one file system to check and what type.
if [[ ${RLV[@]} != "" ]]
then
    print -n "$(date '+%b %e %X') - Node \"$(hostname)\": "
    print "Checking filesystems:"
    print ${LV[@]} | tr ' ' '\012' | sed -e 's/^/   /'

    # If there is more than one filesystem type being checked
    # then each filesystem is check individually.
    #
    R=$(print ${fstype[*]} | tr ' ' '\012' | sort -u | wc -l)
    if (( R > 1 ))
    then
        R=0
        while (( R < ${#RLV[*]} ))
        do
            case ${fstype[$R]} in

                hfs)        fsck -F hfs -P ${RLV[$R]}
                            test_return 2
                            ;;

                vxfs)       fsck -F vxfs -y ${RLV[$R]}
                            test_return 2
                            ;;

                unk*)       fsck ${RLV[$R]}
                            test_return 2
                            ;;

                *)          if [[ ${fstype[$R]} = "" ]]
                            then
                                fsck ${RLV[$R]}
                            else
                                fsck -F ${fstype[$R]} ${RLV[$R]}
                            fi
                            test_return 2
                            ;;
            esac
            (( R = R + 1 ))
        done
```

8357
A.

```
        # If there is only one filesystem type being checked, then
        # multiple invocations of fsck can be avoided. All filesystems
        # are specified on the command line to one fsck invocation.
        #
        else
            case ${fstype} in

                hfs)    fsck -F hfs -P ${RLV[@]}
                        test_return 2
                        ;;

                vxfs)   fsck -F vxfs -y ${RLV[@]}
                        test_return 2
                        ;;

                unk*)   fsck ${RLV[@]}
                        test_return 2
                        ;;

                *)      if [[ ${fstype} = "" ]]
                        then
                            fsck ${RLV[@]}
                        else
                            fsck -F ${fstype} ${RLV[@]}
                        fi
                        test_return 2
                        ;;
            esac
        fi
fi

# Check exit value (set if any proceeding fsck calls failed)

if (( $exit_value == 1 ))
then
        deactivate_volume_group
        print "\n\t############ Node \"$(hostname)\": Package start failed  at $(date)
############"
        exit 1
fi

integer F=0
for I in ${LV[@]}
do
        if [[ $(mount | grep -e $I" ") = "" ]]
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Mounting $I at ${FS[$F]}"
                mount ${FS_MOUNT_OPT[$F]} $I ${FS[$F]}
                test_return 3
        else
                print "$(date '+%b %e %X') - Node \"$(hostname)\": WARNING:  File system
\"${FS[$F]}\" was already mounted."
        fi
        (( F = $F + 1 ))
done
}

# For each {IP address/subnet} pair, add the IP address to the subnet
# using cmmodnet(1m).

function add_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Adding IP address $I to subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -a -i $I ${SUBNET[$S]} 2>&1 )
```


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 252
3698
Doc.

8356
A.

```
        if (( $? != 0 ))
        then
                if [[ $(echo $XX | grep "heartbeat IP") != "" ]]
                then
                        # IP has been configured as a heartbeat IP address.
                        print "$XX" >> $0.log
                        (( error = 1 ))
                else
                        YY=$( netstat -in | awk '$4 == "'${I}'"')
                        if [[ -z $YY ]]
                        then
                                print "$XX" >> $0.log
                                print "\tERROR:  Failed to add IP $I to subnet ${SUBNET[$S]}"
                                (( error = 1 ))
                        else
                                print "\tWARNING:  IP $I is already configured on the subnet
${SUBNET[$S]}"
                        fi
                fi
        fi
        (( S = $S + 1 ))
done

if (( error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 4
fi

}

# Own and reset the DTC connections

function get_ownership_dtc
{
for I in ${DTC_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Assigning Ownership of the DTC $I"
        dtcmodifyconfs -o $I
        test_return 5

        for J in ${IP[@]}
        do
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resetting the DTC
connections to IP address $J"
                dtcdiag -Q $J -q -f $I
                test_return 6
        done
done
}


# For each {service name/service command string} pair, start the
# service command string at the service name using cmrunserv(1m).

function start_services
{
integer C=0
for I in ${SERVICE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting service $I using"
        print "    \"${SERVICE_CMD[$C]}\""
             #
             # Check if cmrunserv should be called the old
             # way without a restart count.
             #
        if [[ "${SERVICE_RESTART[$C]}" = "" ]]
```

```
        then
            cmrunserv $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        else
            cmrunserv ${SERVICE_RESTART[$C]} $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        fi
        test_return 8
        (( C = $C + 1 ))
done
}


# For each {deferred resource name}, start resource monitoring for this
# resource using cmstartres(1m).

function start_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting resource monitoring for
$I"
        cmstartres -u -p $PACKAGE $I >> $0.log 2>&1
        test_return 15
done
}

# END OF RUN FUNCTIONS.


# START OF HALT FUNCTIONS

# For each {deferred resource name}, stop resource monitoring for this
# resource using cmstopres(1m).

function stop_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Stopping resource monitoring for
$I"
        cmstopres -p $PACKAGE $I >> $0.log 2>&1
        test_return 16
done
}


# Halt each service using cmhaltserv(1m).

function halt_services
{
for I in ${SERVICE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Halting service $I"
        cmhaltserv $I
        test_return 9
done
}

# Disown the DTC.

function disown_dtc
{
for I in ${DTC_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Disowning the DTC $I"
        dtcmodifyconfs -d $I
        test_return 11
done
}

# For each IP address/subnet pair, remove the IP address from the subnet
```

8355
A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 253
Doc. 3698

```
# using cmmodnet(1m).
function remove_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Remove IP address $I from subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -r -i $I ${SUBNET[$S]} 2>&1 )
        if (( $? != 0 ))
        then
                echo $XX | grep "is not configured on the subnet"
                if (( $? != 0 ))
                then
                        print "$XX" >> $0.log
                        (( error = 1 ))
                fi
        fi
        (( S = $S + 1 ))
done
if (( $error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 12
fi
}

# Unmount each logical volume.

function umount_fs
{
integer UM_CNT=${FS_UMOUNT_COUNT:-1}

if [[ $UM_CNT < 1 ]]
then
   UM_CNT=1
fi

integer L=${#LV[*]}
while (( L > 0 ))
do
        (( L = L - 1 ))
        I=${LV[$L]}
        mount | grep -e $I" " > /dev/null 2>&1
        if (( $? == 0 ))
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Unmounting filesystem on
$I"
                print "\tWARNING:   Running fuser to remove anyone using the file system
directly."
                UM_COUNT=$UM_CNT
                while (( $UM_COUNT > 0 ))
                do
                fuser -ku $I
                umount $I
                if (( $? == 0 ))
                then
                        (( UM_COUNT = 0 ))
                else
                        if (( $UM_COUNT == 1 ))
                        then
                                let 0
                                test_return 13
                        fi
```

```
                        (( UM_COUNT = $UM_COUNT - 1 ))
                        sleep 1
                        if (( $UM_COUNT > 0 ))
                        then
                                print "\t$(date '+%b %e %X') - Unmount failed, trying again."
                        fi
                fi
                done
        fi
done
}


function deactivate_volume_group
{
for I in ${VG[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Deactivating volume group $I"
        vgchange -a n $I
        test_return 14
done
}

# END OF HALT FUNCTIONS.

# FUNCTIONS COMMON TO BOTH RUN AND HALT.

# Test return value of functions and exit with NO RESTART if bad.
# Return value of 0 - 50 are reserved for use by Hewlett-Packard.
# System administrators can use numbers above 50 for return values.
        function test_return
        {
        if (( $? != 0 ))
        then
                case $1 in
                        1)
                        print "\tERROR:  Function activate_volume_group"
                        print "\tERROR:  Failed to activate $I"
                        deactivate_volume_group
                        exit 1
                        ;;

                        2)
                        print "\tERROR:  Function check_and_mount"
                        print "\tERROR:  Failed to fsck one of the logical volumes."
                        exit_value=1
                        ;;

                        3)
                        print "\tERROR:  Function check_and_mount"
                        print "\tERROR:  Failed to mount $I to ${FS[$F]}"
                        umount_fs
                        deactivate_volume_group
                        exit 1
                        ;;

                        4)
                        print "\tERROR:  Function add_ip_address"
                        print "\tERROR:  Failed to add IP address to subnet"
                        remove_ip_address
                        umount_fs
                        deactivate_volume_group
                        exit 1
                        ;;

                        5)
                        print "\tERROR:  Function get_ownership_dtc"
                        print "\tERROR:  Failed to own $I"
                        disown_dtc
                        remove_ip_address
                        umount_fs
```

8353
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 251
Doc. 3698

8352
A

```
deactivate_volume_group
exit 1
;;

6)
print "\tERROR:  Function get_ownership_dtc"
print "\tERROR:  Failed to switch $I"
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

8)
print "\tERROR:  Function start_services"
print "\tERROR:  Failed to start service ${SERVICE_NAME[$C]}"
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

9)
print "\tFunction halt_services"
print "\tWARNING: Failed to halt service $I"
;;

11)
print "\tERROR:  Function disown_dtc"
print "\tERROR:  Failed to disown $I from ${SUBNET[$S]}"
exit_value=1
;;

12)
print "\tERROR:  Function remove_ip_address"
print "\tERROR:  Failed to remove $I"
exit_value=1
;;

13)
print "\tERROR:  Function umount_fs"
print "\tERROR:  Failed to unmount $I"
exit_value=1
;;

14)
print "\tERROR:  Function deactivate_volume_group"
print "\tERROR:  Failed to deactivate $I"
exit_value=1
;;

15)
print "\tERROR:  Function start_resources"
print "\tERROR:  Failed to start resource $I"
stop_resources
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

16)
print "\tERROR:  Function stop_resources"
print "\tERROR:  Failed to stop resource $I"
```

8351
A-

```
                exit_value=1
                ;;

                51)
                print "\tERROR:  Function customer_defined_run_cmds"
                print "\tERROR:  Failed to RUN customer commands"
                halt_services
                customer_defined_halt_cmds
                disown_dtc
                remove_ip_address
                umount_fs
                deactivate_volume_group
                exit 1
                ;;

                52)
                print "\tERROR:  Function customer_defined_halt_cmds"
                print "\tERROR:  Failed to HALT customer commands"
                exit_value=1
                ;;

                *)
                print "\tERROR:  Failed, unknown error."
                ;;
        esac
fi
}

# END OF FUNCTIONS COMMON TO BOTH RUN AND HALT

#-------------------MAINLINE Control Script Code Starts Here-----------------
#
# FUNCTION STARTUP SECTION.

typeset MIN_VERSION="A.10.03"  # Minimum version this control script works on

integer exit_value=0
typeset CUR_VERSION

#
# Check that this control script is being run on a A.10.03 or later release
# of MC/ServiceGuard or ServiceGuard OPS Edition.  The control scripts are forward
# compatible but are not backward compatible because newer control
# scripts use commands and option not available on older releases.

CUR_VERSION="$(/usr/bin/what /usr/lbin/cmcld | /usr/bin/grep "Date" | \
                        /usr/bin/egrep '[AB]\...\...|NTT\...\...' | \
                        cut -f2 -d" ")"

if [[ "${CUR_VERSION}" = ""  ]] || \
                [[ "${CUR_VERSION#*.}" < "${MIN_VERSION#*.}" ]]
then
    print "ERROR:  Mismatched control script version ($MIN_VERSION).  You cannot run"
    print "\ta version ${MIN_VERSION} control_script on a node running pre"
    print "\t${MIN_VERSION} MC/ServiceGuard or ServiceGuard OPS Edition software"
    exit 1
fi

# Test to see if we are being called to run the package, or halt the package.

if [[ $1 = "start" ]]
then
        print "\n\t############ Node \"$(hostname)\": Starting package at $(date)
############"

        activate_volume_group

        check_and_mount

        add_ip_address
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 255
Doc. 3698

```
                get_ownership_dtc

                customer_defined_run_cmds

                start_services

                start_resources


        # Check exit value

                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package start failed  at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package start completed
at $(date) ############"
                        exit 0
                fi

        elif [[ $1 = "stop" ]]
        then
                print "\n\t############ Node \"$(hostname)\": Halting package at $(date)
############"


                stop_resources

                halt_services

                customer_defined_halt_cmds

                disown_dtc

                remove_ip_address

                umount_fs

                deactivate_volume_group

        # Check exit value
                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package halt failed at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package halt completed at
$(date) ############"
                        exit 0
                fi

fi
```

Appendix 4: OneWorld Xe owpkg2 package configuration file (owpkg2.ascii)

8349
A.

```
# **********************************************************************
# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE (template) *******
# **********************************************************************
# ******* Note: This file MUST be edited before it can be used. ********
# * For complete details about package parameters and how to set them, *
# * consult the MC/ServiceGuard or ServiceGuard OPS Edition manpages   *
# * or manuals.                                                        *
# **********************************************************************

# Enter a name for this package.  This name will be used to identify the
# package when viewing or manipulating it.  It must be different from
# the other configured package names.

PACKAGE_NAME                    owpkg2


# Enter the failover policy for this package. This policy will be used
# to select an adoptive node whenever the package needs to be started.
# The default policy unless otherwise specified is CONFIGURED_NODE.
# This policy will select nodes in priority order from the list of
# NODE_NAME entries specified below.
#
# The alternative policy is MIN_PACKAGE_NODE. This policy will select
# the node, from the list of NODE_NAME entries below, which is
# running the least number of packages at the time this package needs
# to start.

FAILOVER_POLICY                         CONFIGURED_NODE


# Enter the failback policy for this package. This policy will be used
# to determine what action to take when a package is not running on
# its primary node and its primary node is capable of running the
# package. The default policy unless otherwise specified is MANUAL.
# The MANUAL policy means no attempt will be made to move the package
# back to its primary node when it is running on an adoptive node.
#
# The alternative policy is AUTOMATIC. This policy will attempt to
# move the package back to its primary node whenever the primary node
# is capable of running the package.

FAILBACK_POLICY                         MANUAL


# Enter the names of the nodes configured for this package.  Repeat
# this line as necessary for additional adoptive nodes.
# Order IS relevant.  Put the second Adoptive Node AFTER the first
# one.
# Example : NODE_NAME  original_node
#           NODE_NAME  adoptive_node

NODE_NAME                       stxhpc12
NODE_NAME                       stxhpc11


# Enter the complete path for the run and halt scripts.  In most cases
# the run script and halt script specified here will be the same script,
# the package control script generated by the cmmakepkg command.  This
# control script handles the run(ning) and halt(ing) of the package.
# If the script has not completed by the specified timeout value,
# it will be terminated.  The default for each script timeout is
# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full
# execution of each script.
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT                      /etc/cmcluster/owpkg2/control.sh
RUN_SCRIPT_TIMEOUT              NO_TIMEOUT
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 256
Doc. 3698

8348

```
HALT_SCRIPT                     /etc/cmcluster/owpkg2/control.sh
HALT_SCRIPT_TIMEOUT             NO_TIMEOUT

# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names.  All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
# specified SERVICE_HALT_TIMEOUT, the cluster software will send
# out the SIGKILL signal to the service to force its termination.
# This timeout value should be large enough to allow all cleanup
# processes associated with the service to complete.  If the
# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be
# assumed, meaning the cluster software will not wait at all
# before sending the SIGKILL signal to halt the service.
#
# Example: SERVICE_NAME                   DB_SERVICE
#          SERVICE_FAIL_FAST_ENABLED      NO
#          SERVICE_HALT_TIMEOUT           300
#
# To configure a service, uncomment the following lines and
# fill in the values for all of the keywords.
#
#SERVICE_NAME                   <service name>
#SERVICE_FAIL_FAST_ENABLED      <YES/NO>
#SERVICE_HALT_TIMEOUT           <number of seconds>

SERVICE_NAME                    owmonitor2
SERVICE_FAIL_FAST_ENABLED       NO
SERVICE_HALT_TIMEOUT   100


# Enter the network subnet name that is to be monitored for this package.
# Repeat this line as necessary for additional subnet names.  If any of
# the subnets defined goes down, the package will be switched to another
# node that is configured for this package and has all the defined subnets
# available.

SUBNET                  10.225.69.0


# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,
# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify Package
# Resource Dependencies.  To define a package Resource Dependency, a
# RESOURCE_NAME line with a fully qualified resource path name, and
# one or more RESOURCE_UP_VALUE lines are required.  The
# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are optional.
#
# The RESOURCE_POLLING_INTERVAL indicates how often, in seconds, the
# resource is to be monitored.  It will be defaulted to 60 seconds if
# RESOURCE_POLLING_INTERVAL is not specified.
#
# The RESOURCE_START option can be set to either AUTOMATIC or DEFERRED.
# The default setting for RESOURCE_START is AUTOMATIC.  If AUTOMATIC
# is specified, ServiceGuard will start up resource monitoring for
# these AUTOMATIC resources automatically when the node starts up.
```

8347
A.

```
# If DEFERRED is selected, ServiceGuard will not attempt to start
# resource monitoring for these resources during node start up.  User
# should specify all the DEFERRED resources in the package run script
# so that these DEFERRED resources will be started up from the package
# run script during package run time.
#
# RESOURCE_UP_VALUE requires an operator and a value.  This defines
# the resource 'UP' condition.  The operators are =, !=, >, <, >=,
# and <=, depending on the type of value.  Values can be string or
# numeric.  If the type is string, then only = and != are valid
# operators.  If the string contains whitespace, it must be enclosed
# in quotes.  String values are case sensitive.  For example,
#
#                                 Resource is up when its value is
#                                 --------------------------------
#       RESOURCE_UP_VALUE       = UP                    "UP"
#       RESOURCE_UP_VALUE       != DOWN                 Any value except "DOWN"
#       RESOURCE_UP_VALUE       = "On Course"           "On Course"
#
# If the type is numeric, then it can specify a threshold, or a range to
# define a resource up condition.  If it is a threshold, then any operator
# may be used.  If a range is to be specified, then only > or >= may be used
# for the first operator, and only < or <= may be used for the second operator.
# For example,
#                                 Resource is up when its value is
#                                 --------------------------------
#       RESOURCE_UP_VALUE       = 5             5                       (threshold)
#       RESOURCE_UP_VALUE       > 5.1           greater than 5.1        (threshold)
#       RESOURCE_UP_VALUE       > -5 and < 10   between -5 and 10       (range)
#
# Note that "and" is required between the lower limit and upper limit
# when specifying a range.  The upper limit must be greater than the lower
# limit.  If RESOURCE_UP_VALUE is repeated within a RESOURCE_NAME block, then
# they are inclusively OR'd together.  Package Resource Dependencies may be
# defined by repeating the entire RESOURCE_NAME block.
#
# Example : RESOURCE_NAME               /net/interfaces/lan/status/lan0
#           RESOURCE_POLLING_INTERVAL 120
#           RESOURCE_START            AUTOMATIC
#           RESOURCE_UP_VALUE         = RUNNING
#           RESOURCE_UP_VALUE         = ONLINE
#
#           Means that the value of resource /net/interfaces/lan/status/lan0
#           will be checked every 120 seconds, and is considered to
#           be 'up' when its value is "RUNNING" or "ONLINE".
#
# Uncomment the following lines to specify Package Resource Dependencies.
#
#RESOURCE_NAME             <Full_path_name>
#RESOURCE_POLLING_INTERVAL  <numeric_seconds>
#RESOURCE_START             <AUTOMATIC/DEFERRED>
#RESOURCE_UP_VALUE         <op> <string_or_numeric> [and <op> <numeric>]


# The default for PKG_SWITCHING_ENABLED is YES. In the event of a
# failure, this permits the cluster software to transfer the package
# to an adoptive node.  Adjust as necessary.

PKG_SWITCHING_ENABLED          YES


# The default for NET_SWITCHING_ENABLED is YES.  In the event of a
# failure, this permits the cluster software to switch LANs locally
# (transfer to a standby LAN card).  Adjust as necessary.

NET_SWITCHING_ENABLED          YES


# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,
# in the event of a failure, the cluster software will halt the node
# on which the package is running.  Adjust as necessary.
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 257
3698
Doc.

Appendix 5: OneWorld Xe owpkg2 package control file (control.sh)

```
#"(#) A.11.09                                          $Date: 08/06/1999 $"
# **************************************************************************
# *                                                                        *
# *        HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)             *
# *                                                                        *
# *                                                                        *
# **************************************************************************

# UNCOMMENT the variables as you set them.

# Set PATH to reference the appropriate directories.
PATH=/usr/bin:/usr/sbin:/etc:/bin

# VOLUME GROUP ACTIVATION:
# Specify the method of activation for volume groups.
# Leave the default ("VGCHANGE="vgchange -a e") if you want volume
# groups activated in exclusive mode. This assumes the volume groups have
# been initialized with 'vgchange -c y' at the time of creation.
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and comment
# out the default, if your disks are mirrored on separate physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"), and comment
# out the default, if your disks are mirrored on separate physical paths,
# and you want the mirror resynchronization to ocurr in parallel with
# the package startup.
#
# Uncomment the third line (VGCHANGE="vgchange -a y") if you wish to
# use non-exclusive activation mode. Single node cluster configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a e -q n -s"
# VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"              # Default

# VOLUME GROUPS
# Specify which volume groups are used by this package. Uncomment VG[0]=""
# and fill in the name of your first volume group. You must begin with
# VG[0], and increment the list in sequence.
#
# For example, if this package uses your volume groups vg01 and vg02, enter:
#         VG[0]=vg01
#         VG[1]=vg02
#
# The volume group activation method is defined above. The filesystems
# associated with these volume groups are specified below.
#
VG[0]=/dev/vgc12

# FILESYSTEMS
# Specify the filesystems which are used by this package. Uncomment
# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name of your first
# logical volume, filesystem and mount option for the file system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with read and
# write options enter:
#          LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a; FS_MOUNT_OPT[0]="-o rw"
#          LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b; FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying the logical
# volume, the mount point and the mount options for the file system. Each
# filesystem will be fsck'd prior to being mounted. The filesystems will be
# mounted in the order specified during package startup and will be unmounted
# in reverse order during package shutdown. Ensure that volume groups
```


8345
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 258
3698
Doc.

```
# referenced by the logical volume definitions below are included in
# volume group definitions above.
#
LV[0]=/dev/vgcl2/lv01
FS[0]=/u02
FS_MOUNT_OPT[0]=""

# FILESYSTEM UNMOUNT COUNT
# Specify the number of unmount attempts for each filesystem during package
# shutdown.  The default is set to 1.
FS_UMOUNT_COUNT=1

# IP ADDRESSES
# Specify the IP and Subnet address pairs which are used by this package.
# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of your first
# IP and subnet address. You must begin with IP[0] and SUBNET[0] and
# increment the list in sequence.
#
# For example, if this package uses an IP of 192.10.25.12 and a subnet of
# 192.10.25.0 enter:
#          IP[0]=192.10.25.12
#          SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)
#
# Hint: Run "netstat -i" to see the available subnets in the Network field.
#
# IP/Subnet address pairs for each IP address you want to add to a subnet
# interface card.  Must be set in pairs, even for IP addresses on the same
# subnet.
#
IP[0]=10.225.69.23
SUBNET[0]=10.225.69.0

# SERVICE NAMES AND COMMANDS.
# Specify the service name, command, and restart parameters which are
# used by this package. Uncomment SERVICE_NAME[0]="", SERVICE_CMD[0]="",
# SERVICE_RESTART[0]="" and fill in the name of the first service, command,
# and restart parameters. You must begin with SERVICE_NAME[0], SERVICE_CMD[0],
# and SERVICE_RESTART[0] and increment the list in sequence.
#
# For example:
#          SERVICE_NAME[0]=pkg1a
#          SERVICE_CMD[0]="/usr/bin/X11/xclock -display 192.10.25.54:0"
#          SERVICE_RESTART[0]=""  # Will not restart the service.
#
#          SERVICE_NAME[1]=pkg1b
#          SERVICE_CMD[1]="/usr/bin/X11/xload -display 192.10.25.54:0"
#          SERVICE_RESTART[1]="-r 2"   # Will restart the service twice.
#
#          SERVICE_NAME[2]=pkg1c
#          SERVICE_CMD[2]="/usr/sbin/ping"
#          SERVICE_RESTART[2]="-R" # Will restart the service an infinite
#                                  number of times.
#
# Note: No environmental variables will be passed to the command, this
# includes the PATH variable. Absolute path names are required for the
# service command definition.  Default shell is /usr/bin/sh.
#
SERVICE_NAME[0]=owmonitor2
SERVICE_CMD[0]="/etc/cmcluster/owpkg2/monitor.sh"
SERVICE_RESTART[0]="-r 0"
#SERVICE_CMD[0]=""
#SERVICE_RESTART[0]=""

# DEFERRED_RESOURCE NAME
# Specify the full path name of the 'DEFERRED' resources configured for
# this package.  Uncomment DEFERRED_RESOURCE_NAME[0]="" and fill in the
# full path name of the resource.
#
#DEFERRED_RESOURCE_NAME[0]=""

# DTC manager information for each DTC.
```

invent

8343
A1

```
# Example: DTC[0]=dtc_20
#DTC_NAME[0]=


# START OF CUSTOMER DEFINED FUNCTIONS

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# started.  You can create as many functions as you need.

function customer_defined_run_cmds
{
# ADD customer defined run commands.
: # do nothing instruction, because a function must contain some command.

        su owuser1 <<EOF1
        . /u02/oneworld/b733_sp14/system/bin32/owenv
        /u02/oneworld/b733_sp14/system/bin32/RunOneWorld.sh
EOF1

        test_return 51
}

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# halted.

function customer_defined_halt_cmds
{
# ADD customer defined halt commands.
: # do nothing instruction, because a function must contain some command.

        su owuser1 <<EOF2
        . /u02/oneworld/b733_sp14/system/bin32/owenv
        /u02/oneworld/b733_sp14/system/bin32/EndOneWorld.sh now
EOF2

        test_return 52
}

# END OF CUSTOMER DEFINED FUNCTIONS


# START OF RUN FUNCTIONS


function activate_volume_group
{
for I in ${VG[@]}
do
        if [[ "${VGCHANGE}" = "vgchange -a y" ]]
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Activating volume group $I
with non-exclusive option."
        else
                print "$(date '+%b %e %X') - \"$(hostname)\": Activating volume group $I with
exclusive option."
        fi

        $VGCHANGE $I
        test_return 1

        # If the -s option has been specified, then we perform
        # the resynchronization as a background task
        #
        if [[ ${VGCHANGE#*-s} != ${VGCHANGE} ]]
        then
            {
                if /sbin/vgsync $I
                then
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 259
Doc. 3698

8542 A.

```
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronized volume
group $I"
            else
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronization of
volume group $I encountered an error"
            fi
        } &
    fi
done
}

# For each {file system/logical volume} pair, fsck the file system
# and mount it.  If the file system is busy, mounting of the file
# system will fail, the control script will exit with an error.

function check_and_mount
{
integer R=0

for I in ${LV[@]}
do
    if [[ $(mount -p | awk '$1 == "'$I'"') = "" ]]
    then
        RLV[$R]="${I%/*}/r${I##*/}"

        if [ -x /usr/sbin/fstyp ]
        then
                fstype[$R]=$(fstyp $I)
        fi
        (( R = $R + 1 ))
    fi
done

# Verify that there is at least one file system to check and what type.
if [[ ${RLV[@]} != "" ]]
then
    print -n "$(date '+%b %e %X') - Node \"$(hostname)\": "
    print "Checking filesystems:"
    print ${LV[@]} | tr ' ' '\012' | sed -e 's/^/   /'

    # If there is more than one filesystem type being checked
    # then each filesystem is check individually.
    #
    R=$(print ${fstype[*]} | tr ' ' '\012' | sort -u | wc -l)
    if (( R > 1 ))
    then
        R=0
        while (( R < ${#RLV[*]} ))
        do
            case ${fstype[$R]} in

                hfs)        fsck -F hfs -P ${RLV[$R]}
                            test_return 2
                            ;;

                vxfs)       fsck -F vxfs -y ${RLV[$R]}
                            test_return 2
                            ;;

                unk*)       fsck ${RLV[$R]}
                            test_return 2
                            ;;

                *)          if [[ ${fstype[$R]} = "" ]]
                            then
                                fsck ${RLV[$R]}
                            else
                                fsck -F ${fstype[$R]} ${RLV[$R]}
                            fi
                            test_return 2
                            ;;
```

```
                esac
                (( R = R + 1 ))
            done

        # If there is only one filesystem type being checked, then
        # multiple invocations of fsck can be avoided. All filesystems
        # are specified on the command line to one fsck invocation.
        #
        else
            case ${fstype} in

                hfs)    fsck -F hfs -P ${RLV[@]}
                        test_return 2
                        ;;

                vxfs)   fsck -F vxfs -y ${RLV[@]}
                        test_return 2
                        ;;

                unk*)   fsck ${RLV[@]}
                        test_return 2
                        ;;

                *)      if [[ ${fstype} = "" ]]
                        then
                            fsck ${RLV[@]}
                        else
                            fsck -F ${fstype} ${RLV[@]}
                        fi
                        test_return 2
                        ;;
            esac
        fi
fi

# Check exit value (set if any proceeding fsck calls failed)

if (( $exit_value == 1 ))
then
        deactivate_volume_group
        print "\n\t############ Node \"$(hostname)\": Package start failed  at $(date)
############"
        exit 1
fi

integer F=0
for I in ${LV[@]}
do
        if [[ $(mount | grep -e $I" ") = "" ]]
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Mounting $I at ${FS[$F]}"
                mount ${FS_MOUNT_OPT[$F]} $I ${FS[$F]}
                test_return 3
        else
                print "$(date '+%b %e %X') - Node \"$(hostname)\": WARNING:  File system
\"${FS[$F]}\" was already mounted."
        fi
        (( F = $F + 1 ))
done
}

# For each {IP address/subnet} pair, add the IP address to the subnet
# using cmmodnet(1m).

function add_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
```

8341
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 200
Doc. 3698

```
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Adding IP address $I to subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -a -i $I ${SUBNET[$S]} 2>&1 )
        if (( $? != 0 ))
        then
                if [[ $(echo $XX | grep "heartbeat IP") != "" ]]
                then
                        # IP has been configured as a heartbeat IP address.
                        print "$XX" >> $0.log
                        (( error = 1 ))
                else
                        YY=$( netstat -in | awk '$4 == "'${I}'"')
                        if [[ -z $YY ]]
                        then
                                print "$XX" >> $0.log
                                print "\tERROR:  Failed to add IP $I to subnet ${SUBNET[$S]}"
                                (( error = 1 ))
                        else
                                print "\tWARNING:  IP $I is already configured on the subnet
${SUBNET[$S]}"
                        fi
                fi
        fi
        (( S = $S + 1 ))
done

if (( error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 4
fi

}

# Own and reset the DTC connections

function get_ownership_dtc
{
for I in ${DTC_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Assigning Ownership of the DTC $I"
        dtcmodifyconfs -o $I
        test_return 5

        for J in ${IP[@]}
        do
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resetting the DTC
connections to IP address $J"
                dtcdiag -Q $J -q -f $I
                test_return 6
        done
done
}


# For each {service name/service command string} pair, start the
# service command string at the service name using cmrunserv(1m).

function start_services
{
integer C=0
for I in ${SERVICE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting service $I using"
        print "    \"${SERVICE_CMD[$C]}\""
             #
             # Check if cmrunserv should be called the old
```

```
            # way without a restart count.
            #
        if [[ "${SERVICE_RESTART[$C]}" = "" ]]
        then
            cmrunserv $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        else
            cmrunserv ${SERVICE_RESTART[$C]} $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        fi
        test_return 8
        (( C = $C + 1 ))
done
}


# For each {deferred resource name}, start resource monitoring for this
# resource using cmstartres(1m).

function start_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting resource monitoring for
$I"
        cmstartres -u -p $PACKAGE $I >> $0.log 2>&1
        test_return 15
done
}

# END OF RUN FUNCTIONS.


# START OF HALT FUNCTIONS

# For each {deferred resource name}, stop resource monitoring for this
# resource using cmstopres(1m).

function stop_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Stopping resource monitoring for
$I"
        cmstopres -p $PACKAGE $I >> $0.log 2>&1
        test_return 16
done
}


# Halt each service using cmhaltserv(1m).

function halt_services
{
for I in ${SERVICE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Halting service $I"
        cmhaltserv $I
        test_return 9
done
}

# Disown the DTC.

function disown_dtc
{
for I in ${DTC_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Disowning the DTC $I"
        dtcmodifyconfs -d $I
        test_return 11
done
```

8339
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 261
Doc. 3698

8338 A.

```
}

# For each IP address/subnet pair, remove the IP address from the subnet
# using cmmodnet(1m).

function remove_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Remove IP address $I from subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -r -i $I ${SUBNET[$S]} 2>&1 )
        if (( $? != 0 ))
        then
                echo $XX | grep "is not configured on the subnet"
                if (( $? != 0 ))
                then
                        print "$XX" >> $0.log
                        (( error = 1 ))
                fi
        fi
        (( S = $S + 1 ))
done
if (( $error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 12
fi
}

# Unmount each logical volume.

function umount_fs
{
integer UM_CNT=${FS_UMOUNT_COUNT:-1}

if [[ $UM_CNT < 1 ]]
then
   UM_CNT=1
fi

integer L=${#LV[*]}
while (( L > 0 ))
do
        (( L = L - 1 ))
        I=${LV[$L]}
        mount | grep -e $I" " > /dev/null 2>&1
        if (( $? == 0 ))
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Unmounting filesystem on
$I"
                print "\tWARNING:   Running fuser to remove anyone using the file system
directly."
                UM_COUNT=$UM_CNT
                while (( $UM_COUNT > 0 ))
                do
                fuser -ku $I
                umount $I
                if (( $? == 0 ))
                then
                        (( UM_COUNT = 0 ))
                else
                        if (( $UM_COUNT == 1 ))
                        then
```

```
                        let 0
                        test_return 13
                fi
                (( UM_COUNT = $UM_COUNT - 1 ))
                sleep 1
                if (( $UM_COUNT > 0 ))
                then
                        print "\t$(date '+%b %e %X') - Unmount failed, trying again."
                fi
        fi
        done
    fi
done
}


function deactivate_volume_group
{
for I in ${VG[@]}
do
    print "$(date '+%b %e %X') - Node \"$(hostname)\": Deactivating volume group $I"
    vgchange -a n $I
    test_return 14
done
}

# END OF HALT FUNCTIONS.

# FUNCTIONS COMMON TO BOTH RUN AND HALT.

# Test return value of functions and exit with NO RESTART if bad.
# Return value of 0 - 50 are reserved for use by Hewlett-Packard.
# System administrators can use numbers above 50 for return values.
    function test_return
    {
    if (( $? != 0 ))
    then
        case $1 in
            1)
            print "\tERROR:  Function activate_volume_group"
            print "\tERROR:  Failed to activate $I"
            deactivate_volume_group
            exit 1
            ;;

            2)
            print "\tERROR:  Function check_and_mount"
            print "\tERROR:  Failed to fsck one of the logical volumes."
            exit_value=1
            ;;

            3)
            print "\tERROR:  Function check_and_mount"
            print "\tERROR:  Failed to mount $I to ${FS[$F]}"
            umount_fs
            deactivate_volume_group
            exit 1
            ;;

            4)
            print "\tERROR:  Function add_ip_address"
            print "\tERROR:  Failed to add IP address to subnet"
            remove_ip_address
            umount_fs
            deactivate_volume_group
            exit 1
            ;;

            5)
            print "\tERROR:  Function get_ownership_dtc"
            print "\tERROR:  Failed to own $I"
```


8337
A.

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 262
3698
Doc.

8336 A

```
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

6)
print "\tERROR:  Function get_ownership_dtc"
print "\tERROR:  Failed to switch $I"
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

8)
print "\tERROR:  Function start_services"
print "\tERROR:  Failed to start service ${SERVICE_NAME[$C]}"
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

9)
print "\tFunction halt_services"
print "\tWARNING: Failed to halt service $I"
;;

11)
print "\tERROR:  Function disown_dtc"
print "\tERROR:  Failed to disown $I from ${SUBNET[$S]}"
exit_value=1
;;

12)
print "\tERROR:  Function remove_ip_address"
print "\tERROR:  Failed to remove $I"
exit_value=1
;;

13)
print "\tERROR:  Function umount_fs"
print "\tERROR:  Failed to unmount $I"
exit_value=1
;;

14)
print "\tERROR:  Function deactivate_volume_group"
print "\tERROR:  Failed to deactivate $I"
exit_value=1
;;

15)
print "\tERROR:  Function start_resources"
print "\tERROR:  Failed to start resource $I"
stop_resources
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;
```

8335
A.

```
                16)
                print "\tERROR:  Function stop_resources"
                print "\tERROR:  Failed to stop resource $I"
                exit_value=1
                ;;

                51)
                print "\tERROR:  Function customer_defined_run_cmds"
                print "\tERROR:  Failed to RUN customer commands"
                halt_services
                customer_defined_halt_cmds
                disown_dtc
                remove_ip_address
                umount_fs
                deactivate_volume_group
                exit 1
                ;;

                52)
                print "\tERROR:  Function customer_defined_halt_cmds"
                print "\tERROR:  Failed to HALT customer commands"
                exit_value=1
                ;;

                *)
                print "\tERROR:  Failed, unknown error."
                ;;
        esac
fi
}

# END OF FUNCTIONS COMMON TO BOTH RUN AND HALT

#------------------MAINLINE Control Script Code Starts Here----------------
#
# FUNCTION STARTUP SECTION.

typeset MIN_VERSION="A.10.03"  # Minimum version this control script works on

integer exit_value=0
typeset CUR_VERSION

#
# Check that this control script is being run on a A.10.03 or later release
# of MC/ServiceGuard or ServiceGuard OPS Edition.  The control scripts are forward
# compatible but are not backward compatible because newer control
# scripts use commands and option not available on older releases.

CUR_VERSION="$(/usr/bin/what /usr/lbin/cmcld | /usr/bin/grep "Date" | \
                        /usr/bin/egrep '[AB]\...\...|NTT\...\...' | \
                        cut -f2 -d" ")"

if [[ "${CUR_VERSION}" = ""  ]] || \
                        [[ "${CUR_VERSION#*.}" < "${MIN_VERSION#*.}" ]]
then
    print "ERROR:  Mismatched control script version ($MIN_VERSION).  You cannot run"
    print "\ta version ${MIN_VERSION} control_script on a node running pre"
    print "\t${MIN_VERSION} MC/ServiceGuard or ServiceGuard OPS Edition software"
    exit 1
fi

# Test to see if we are being called to run the package, or halt the package.

if [[ $1 = "start" ]]
then
        print "\n\t############ Node \"$(hostname)\": Starting package at $(date)
############"

        activate_volume_group

        check_and_mount
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 263
3698
Doc.

```
                add_ip_address

                get_ownership_dtc

                customer_defined_run_cmds

                start_services

                start_resources


        # Check exit value

                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package start failed  at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package start completed
at $(date) ############"
                        exit 0
                fi

        elif [[ $1 = "stop" ]]
        then
                print "\n\t############ Node \"$(hostname)\": Halting package at $(date)
############"


                stop_resources

                halt_services

                customer_defined_halt_cmds

                disown_dtc

                remove_ip_address

                umount_fs

                deactivate_volume_group

        # Check exit value
                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package halt failed at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package halt completed at
$(date) ############"
                        exit 0
                fi

fi
```

Appendix 6: OneWorld Xe Monitor Script (monitor.sh) (same script for each package)

```
#!/bin/ksh

sleep 30
USER="owuser1"
CHECKFOR="jdenet_n jdequeue"

trap "exit" 15

while true
do
        for i in $CHECKFOR
        do
                print ""
                print "checking for process $i"
                ps -ef | grep $i | grep $USER | grep -v grep > /dev/null 2>&1
                if [ $? -ne 0 ]
                then
                        print "\n"
                        print "exiting monitor script - process $i not found"
                        exit 1
                fi
        done
        sleep 15
done
```

B333
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 264
Doc. 3698

8332 A.

Appendix 7: Output of <bdf> on node stxhpcl1

```
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   28396  107830   21% /
/dev/vg00/lvol1      83733   27523   47836   37% /stand
/dev/vg00/lvol8     512000  304403  195643   61% /var
/dev/vg00/lvol7     512000  381535  122314   76% /usr
/dev/vg00/lvol4      65536    1130   60384    2% /tmp
/dev/vg00/lvol6     348160   63771  266678   19% /opt
/dev/vg00/lvol5      20480    1351   17988    7% /home
/dev/vg01/lv01     4096000 1238276 2679117   32% /u01
/dev/vgcl1/lv01   16384000 2111310 13826718   13% /u03
```

Appendix 8: Output of <bdf> on node stxhpcl2

```
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   67656   71009   49% /
/dev/vg00/lvol1      83733   27523   47836   37% /stand
/dev/vg00/lvol8     512000  306623  193514   61% /var
/dev/vg00/lvol7     512000  381550  122299   76% /usr
/dev/vg00/lvol4      65536    1272   60314    2% /tmp
/dev/vg00/lvol6     348160  170584  166492   51% /opt
/dev/vg00/lvol5      20480    1348   17991    7% /home
/dev/vg01/lv01     4096000  447897 3420097   12% /u01
/dev/vgcl2/lv01   16384000 2903542 13059198   18% /u02
```

Appendix 9: Output of <cmviewcl -v>

```
CLUSTER      STATUS
hpcluster    up

  NODE         STATUS       STATE
  stxhpcl1     up           running

    Network_Parameters:
    INTERFACE    STATUS       PATH         NAME
    PRIMARY      up           10/12/6      lan0

    PACKAGE      STATUS       STATE        PKG_SWITCH   NODE
    owpkg1       up           running      enabled      stxhpcl1

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM       STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service    up                0          0   owmonitor
      Subnet     up                               10.225.69.0
      Resource   up                               /system/filesystem/availMb/tmp

      Node_Switching_Parameters:
      NODE_TYPE    STATUS       SWITCHING    NAME
      Primary      up           enabled      stxhpcl1     (current)
      Alternate    up           enabled      stxhpcl2

  NODE         STATUS       STATE
  stxhpcl2     up           running

    Network_Parameters:
    INTERFACE    STATUS       PATH         NAME
    PRIMARY      up           10/12/6      lan0

    PACKAGE      STATUS       STATE        PKG_SWITCH   NODE
    owpkg2       up           running      enabled      stxhpcl2

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM       STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service    up                0          0   owmonitor2
      Subnet     up                               10.225.69.0

      Node_Switching_Parameters:
      NODE_TYPE    STATUS       SWITCHING    NAME
      Primary      up           enabled      stxhpcl2     (current)
      Alternate    up           enabled      stxhpcl1
```

8331

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 2659
Doc. 3698

8330

Appendix 10: Contents of /etc/fstab on node stxhpcl1

```
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs defaults 0 1
/dev/vg00/lvol4 /tmp vxfs delaylog 0 2
/dev/vg00/lvol5 /home vxfs delaylog 0 2
/dev/vg00/lvol6 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
#/dev/vgcl/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv02 /u02 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv03 /u03 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv04 /u04 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vg01/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vgcl1/lv01 /u03 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
```

Appendix 11: Contents of /etc/fstab on node stxhpcl2

```
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs defaults 0 1
/dev/vg00/lvol4 /tmp vxfs delaylog 0 2
/dev/vg00/lvol5 /home vxfs delaylog 0 2
/dev/vg00/lvol6 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
#/dev/vgcl/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv02 /u02 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv03 /u03 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv04 /u04 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vg01/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vgcl2/lv01 /u02 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
```

Appendix 12: Contents of /etc/hosts

8329
A.

```
# @(#)hosts $Revision: 1.9.214.1 $ $Date: 96/10/08 13:20:01 $
#
# The form for each entry is:
# <internet address>   <official hostname> <aliases>
#
# For example:
# 192.1.2.34   hpfcrm  loghost
#
# See the hosts(4) manual page for more information.
# Note: The entries cannot be preceded by a space.
#       The format described in this file is the correct format.
#       The original Berkeley manual page contains an error in
#       the format description.
#

10.225.69.20    stxhpcl1
127.0.0.1       localhost       loopback
10.225.69.21    stxhpcl2

10.225.69.22    hpcluster
10.225.69.23    hpcluster2

10.0.40.73      corowsn1
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 260
3693
Doc.

Appendix 13: Output of <ioscan -f>

8320 A

```
Class     I  H/W Path     Driver       S/W State H/W Type  Description
=============================================================================
bc        0                root         CLAIMED   BUS_NEXUS
bc        1  8             ccio         CLAIMED   BUS_NEXUS I/O Adapter
bc        2  10            ccio         CLAIMED   BUS_NEXUS I/O Adapter
ext_bus   0  10/0          c720         CLAIMED   INTERFACE GSC built-in Fast/Wide SCSI
Interface
target    0  10/0.1        tgt          CLAIMED   DEVICE
disk      0  10/0.1.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    1  10/0.3        tgt          CLAIMED   DEVICE
disk      1  10/0.3.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    2  10/0.4        tgt          CLAIMED   DEVICE
disk      2  10/0.4.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    3  10/0.5        tgt          CLAIMED   DEVICE
disk      3  10/0.5.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    4  10/0.6        tgt          CLAIMED   DEVICE
disk      4  10/0.6.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    5  10/0.7        tgt          CLAIMED   DEVICE
ctl       0  10/0.7.0      sctl         CLAIMED   DEVICE    Initiator
target    6  10/0.9        tgt          CLAIMED   DEVICE
disk      5  10/0.9.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    7  10/0.10       tgt          CLAIMED   DEVICE
disk      6  10/0.10.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target    8  10/0.11       tgt          CLAIMED   DEVICE
disk      7  10/0.11.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
bc        3  10/4          bc           CLAIMED   BUS_NEXUS Bus Converter
tty       0  10/4/0        mux2         CLAIMED   INTERFACE MUX
ext_bus   1  10/8          c720         CLAIMED   INTERFACE GSC add-on Fast/Wide SCSI
Interface
target    9  10/8.0        tgt          CLAIMED   DEVICE
disk      8  10/8.0.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   10  10/8.3        tgt          CLAIMED   DEVICE
disk      9  10/8.3.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   11  10/8.4        tgt          CLAIMED   DEVICE
disk     10  10/8.4.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   12  10/8.5        tgt          CLAIMED   DEVICE
disk     11  10/8.5.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   13  10/8.6        tgt          CLAIMED   DEVICE
disk     12  10/8.6.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   14  10/8.12       tgt          CLAIMED   DEVICE
disk     13  10/8.12.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   15  10/8.13       tgt          CLAIMED   DEVICE
disk     14  10/8.13.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   16  10/8.14       tgt          CLAIMED   DEVICE
disk     15  10/8.14.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target   17  10/8.15       tgt          CLAIMED   DEVICE
ctl       1  10/8.15.0     sctl         CLAIMED   DEVICE    Initiator
ba        0  10/12         bus_adapter  CLAIMED   BUS_NEXUS Core I/O Adapter
ext_bus   3  10/12/0       CentIf       CLAIMED   INTERFACE Built-in Parallel Interface
ext_bus   2  10/12/5       c720         CLAIMED   INTERFACE Built-in SCSI
target   18  10/12/5.0      tgt          CLAIMED   DEVICE
tape      0  10/12/5.0.0    stape        CLAIMED   DEVICE    HP      C1533A
target   19  10/12/5.2      tgt          CLAIMED   DEVICE
disk     16  10/12/5.2.0    sdisk        CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5701TA
target   20  10/12/5.7      tgt          CLAIMED   DEVICE
ctl       2  10/12/5.7.0    sctl         CLAIMED   DEVICE    Initiator
lan       0  10/12/6        lan2         CLAIMED   INTERFACE Built-in LAN
ps2       0  10/12/7        ps2          CLAIMED   INTERFACE Built-in Keyboard/Mouse
processor 0  32             processor    CLAIMED   PROCESSOR Processor
processor 1  34             processor    CLAIMED   PROCESSOR Processor
memory    0  49             memory       CLAIMED   MEMORY    Memory
```

Appendix 14: Output of <lanscan>

```
Hardware Station         Crd Hdw   Net-Interface  NM  MAC       HP-DLPI DLPI
Path     Address         In# State NamePPA        ID  Type      Support Mjr#
10/12/6  0x0060B032AA2F  0   UP    lan0 snap0     1   ETHER     Yes     119
```

8327
A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 267
Doc. 3698

8326 A

Appendix 15: Contents of /etc/lvmrc

```
# "@(#)/etc/lvmrc       $Revision: 72.2 $$Date: 94/05/20 17:46:54 $"
#
# This file is sourced by /sbin/lvmrc. This file contains the flags
# AUTO_VG_ACTIVATE and RESYNC which are required by the script in /sbin/lvmrc.
# These flags must be set to valid values (see below).
#
#
# The activation of Volume Groups may be customized by setting the
# AUTO_VG_ACTIVATE flag to 0 and customizing the function
# custom_vg_activation()
#

#
#       To disable automatic volume group activation,
#       set AUTO_VG_ACTIVATE to 0.
#

AUTO_VG_ACTIVATE=0

#
#       The variable RESYNC controls the order in which
#       Volume Groups are resyncronized. Allowed values
#       are:
#               "PARALLEL"      - resync all VGs at once.
#               "SERIAL"        - resync VGs one at a time.
#
#       SERIAL will take longer but will have less of an
#       impact on overall I/O performance.
#

RESYNC="SERIAL"


#
#       Add customized volume group activation here.
#       A function is available that will synchronize all
#       volume groups in a list in parallel. It is
#       called parallel_vg_sync.
#
#       This routine is only executed if AUTO_VG_ACTIVATE
#       equals 0.
#

custom_vg_activation()
{
        # e.g. /sbin/vgchange -a y -s
        #      parallel_vg_sync "/dev/vg00 /dev/vg01"
        #      parallel_vg_sync "/dev/vg02 /dev/vg03"

        return 0
}

#
# The following functions should require no additional customization:
#

parallel_vg_sync()
{
        for VG in $*
        do
                {
                if /sbin/vgsync $VG > /dev/null
                then
                        echo "Resynchronized volume group $VG"
                fi
                } &
        done
}
```

Appendix 16: Output of </etc/mount> on stxhpcl1

```
/ on /dev/vg00/lvol3 log on Mon Oct  9 15:57:01 2000
/stand on /dev/vg00/lvol1 defaults on Mon Oct  9 15:57:04 2000
/var on /dev/vg00/lvol8 delaylog,nodatainlog on Mon Oct  9 15:57:18 2000
/usr on /dev/vg00/lvol7 delaylog,nodatainlog on Mon Oct  9 15:57:18 2000
/tmp on /dev/vg00/lvol4 delaylog,nodatainlog on Mon Oct  9 15:57:18 2000
/opt on /dev/vg00/lvol6 delaylog,nodatainlog on Mon Oct  9 15:57:19 2000
/home on /dev/vg00/lvol5 delaylog,nodatainlog on Mon Oct  9 15:57:19 2000
/u01 on /dev/vg01/lv01 delaylog,nodatainlog on Tue Oct 10 09:58:45 2000
/u03 on /dev/vgcl1/lv01 log,nodatainlog on Wed Oct 11 14:40:29 2000
```

Appendix 17: Output of </etc/mount> on stxhpcl2

```
/ on /dev/vg00/lvol3 log on Mon Oct  9 15:52:35 2000
/stand on /dev/vg00/lvol1 defaults on Mon Oct  9 15:52:37 2000
/var on /dev/vg00/lvol8 delaylog,nodatainlog on Mon Oct  9 15:52:51 2000
/usr on /dev/vg00/lvol7 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/tmp on /dev/vg00/lvol4 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/opt on /dev/vg00/lvol6 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/home on /dev/vg00/lvol5 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/u01 on /dev/vg01/lv01 delaylog,nodatainlog on Tue Oct 10 10:24:35 2000
/u02 on /dev/vgcl2/lv01 log,nodatainlog on Wed Oct 11 13:32:12 2000
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 208
3698
Doc.

Appendix 18: Contents of /etc/rc.config.d/netconf on stxhpcl1

```
# netconf:  configuration values for core networking subsystems
#
# @(#) $Revision: 1.6.119.6 $ $Date: 97/09/10 15:56:01 $
#
# HOSTNAME:            Name of your system for uname -S and hostname
#
# OPERATING_SYSTEM:    Name of operating system returned by uname -s
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# LOOPBACK_ADDRESS:    Loopback address
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

HOSTNAME="stxhpcl1"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

# Internet configuration parameters.  See ifconfig(1m), autopush(1m)
#
# INTERFACE_NAME:      Network interface name (see lanscan(1m))
#
# IP_ADDRESS:          Hostname (in /etc/hosts) or IP address in decimal-dot
#                      notation (e.g., 192.1.2.3)
#
# SUBNET_MASK:         Subnetwork mask in decimal-dot notation, if different
#                      from default
#
# BROADCAST_ADDRESS:   Broadcast address in decimal-dot notation, if
#                      different from default
#
# INTERFACE_STATE:     Desired interface state at boot time.
#                      either up or down, default is up.
#
# DHCP_ENABLE          Determines whether or not DHCP client functionality
#                      will be enabled on the network interface (see
#                      auto_parms(1M), dhcpclient(1M)). DHCP clients get
#                      their IP address assignments from DHCP servers.
#                      1 enables DHCP client functionality; 0 disables it.
#
# For each additional network interfaces, add a set of variable assignments
# like the ones below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

INTERFACE_NAME[0]="lan0"
IP_ADDRESS[0]="10.225.69.20"
SUBNET_MASK[0]="255.255.255.0"
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0

# Internet routing configuration.  See route(1m), routing(7)
#
# ROUTE_DESTINATION:   Destination hostname (in /etc/hosts) or host or network
#                      IP address in decimal-dot notation, preceded by the word
#                      "host" or "net"; or simply the word "default".
#
# ROUTE_MASK:          Subnetwork mask in decimal-dot notation, or C language
#                      hexadecimal notation.  This is an optional field.
#                      A IP address, subnet mask pair uniquely identifies
#                      a subnet to be reached. If a subnet mask is not given,
#                      then the system will assign the longest subnet mask
#                      of the configured network interfaces to this route.
#                      If there is no matching subnet mask, then the system
```

```
#                       will assign the default network mask as the route's
#                       subnet mask.
#
# ROUTE_GATEWAY:        Gateway hostname (in /etc/hosts) or IP address in
#                       decimal-dot notation.  If local interface, must use the
#                       same form as used for IP_ADDRESS above (hostname or
#                       decimal-dot notation). If loopback interface, i.e.,
#                      127.0.0.1, the ROUTE_COUNT must be set to zero.
#
# ROUTE_COUNT:          An integer that indicates whether the gateway is a
#                       remote interface (one) or the local interface (zero)
#                      or loopback interface (e.g., 127.*).
#
# ROUTE_ARGS:           Route command arguments and options.  This variable
#                       may contain a combination of the following arguments:
#                       "-f", "-n" and "-p pmtu".
#
# For each additional route, add a set of variable assignments like the ones
# below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

ROUTE_DESTINATION[0]="default"
ROUTE_MASK[0]=""
ROUTE_GATEWAY[0]="10.225.69.20"
ROUTE_COUNT[0]="0"
ROUTE_ARGS[0]=""

# Dynamic routing daemon configuration.  See gated(1m)
#
# GATED:        Set to 1 to start gated daemon.
# GATED_ARGS:   Arguments to the gated daemon.

GATED=0
GATED_ARGS=""

#
# Router Discover Protocol daemon configuration.  See rdpd(1m)
#
# RDPD:         Set to 1 to start rdpd daemon
#

RDPD=0

#
# Reverse ARP daemon configuration.  See rarpd(1m)
#
# RARP:         Set to 1 to start rarpd daemon
#

RARP=0
```

8322
A.

RDC nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 269
3698
Doc.

Appendix 19: Contents of /etc/rc.config.d/netconf on stxhpcl2

```
# netconf:Configuration values for core networking subsystems
#
# @(#) $Revision: 1.6.119.6 $ $Date: 97/09/10 15:56:01 $
#
# HOSTNAME:            Name of your system for uname -S and hostname
#
# OPERATING_SYSTEM:    Name of operating system returned by uname -s
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# LOOPBACK_ADDRESS:    Loopback address
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

HOSTNAME="stxhpcl2"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

# Internet configuration parameters.  See ifconfig(1m), autopush(1m)
#
# INTERFACE_NAME:      Network interface name (see lanscan(1m))
#
# IP_ADDRESS:          Hostname (in /etc/hosts) or IP address in decimal-dot
#                      notation (e.g., 192.1.2.3)
#
# SUBNET_MASK:         Subnetwork mask in decimal-dot notation, if different
#                      from default
#
# BROADCAST_ADDRESS:   Broadcast address in decimal-dot notation, if
#                      different from default
#
# INTERFACE_STATE:     Desired interface state at boot time.
#                      either up or down, default is up.
#
# DHCP_ENABLE          Determines whether or not DHCP client functionality
#                      will be enabled on the network interface (see
#                      auto_parms(1M), dhcpclient(1M)). DHCP clients get
#                      their IP address assignments from DHCP servers.
#                      1 enables DHCP client functionality; 0 disables it.
#
# For each additional network interfaces, add a set of variable assignments
# like the ones below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

INTERFACE_NAME[0]=lan0
IP_ADDRESS[0]=10.225.69.21
SUBNET_MASK[0]=255.255.255.0
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0

# Internet routing configuration.  See route(1m), routing(7)
#
# ROUTE_DESTINATION:   Destination hostname (in /etc/hosts) or host or network
#                      IP address in decimal-dot notation, preceded by the word
#                      "host" or "net"; or simply the word "default".
#
# ROUTE_MASK:          Subnetwork mask in decimal-dot notation, or C language
#                      hexadecimal notation.  This is an optional field.
#                      A IP address, subnet mask pair uniquely identifies
#                      a subnet to be reached. If a subnet mask is not given,
#                      then the system will assign the longest subnet mask
#                      of the configured network interfaces to this route.
#                      If there is no matching subnet mask, then the system
#                      will assign the default network mask as the route's
```

```
#                       subnet mask.
#
# ROUTE_GATEWAY:        Gateway hostname (in /etc/hosts) or IP address in
#                       decimal-dot notation.  If local interface, must use the
#                       same form as used for IP_ADDRESS above (hostname or
#                       decimal-dot notation). If loopback interface, i.e.,
#                      127.0.0.1, the ROUTE_COUNT must be set to zero.
#
# ROUTE_COUNT:          An integer that indicates whether the gateway is a
#                       remote interface (one) or the local interface (zero)
#                      or loopback interface (e.g., 127.*).
#
# ROUTE_ARGS:           Route command arguments and options.  This variable
#                       may contain a combination of the following arguments:
#                       "-f", "-n" and "-p pmtu".
#
# For each additional route, add a set of variable assignments like the ones
# below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

# ROUTE_DESTINATION[0]=default
# ROUTE_MASK[0]=""
# ROUTE_GATEWAY[0]=""
# ROUTE_COUNT[0]=""
# ROUTE_ARGS[0]=""

# Dynamic routing daemon configuration.  See gated(1m)
#
# GATED:        Set to 1 to start gated daemon.
# GATED_ARGS:   Arguments to the gated daemon.

GATED=0
GATED_ARGS=""

#
# Router Discover Protocol daemon configuration.  See rdpd(1m)
#
# RDPD:         Set to 1 to start rdpd daemon
#

RDPD=0

#
# Reverse ARP daemon configuration.  See rarpd(1m)
#
# RARP:         Set to 1 to start rarpd daemon
#

RARP=0

ROUTE_GATEWAY[0]=10.225.69.21
ROUTE_COUNT[0]=0
ROUTE_DESTINATION[0]=default
```

8320
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 270
Doc. 3698

8319

Appendix 20: Output of <netstat -nr> on stxhpcl1

```
Routing tables
Dest/Netmask            Gateway             Flags   Refs       Use   Interface   Pmtu
127.0.0.1               127.0.0.1           UH         0     95871   lo0         4136
10.225.69.20            10.225.69.20        UH         0     18413   lan0        4136
10.225.69.22            10.225.69.22        UH         0         0   lan0:1      4136
10.225.69.0             10.225.69.20        U          3         0   lan0        1500
10.225.69.0             10.225.69.22        U          3         0   lan0:1      1500
127.0.0.0               127.0.0.1           U          0         0   lo0         4136
default                 10.225.69.20        U          0         0   lan0        1500
```

Appendix 21: Output of <netstat -nr> on stxhpcl2

```
Routing tables
Dest/Netmask            Gateway             Flags   Refs       Use   Interface   Pmtu
127.0.0.1               127.0.0.1           UH         0     73359   lo0         4136
10.225.69.21            10.225.69.21        UH         0     11695   lan0        4136
10.225.69.23            10.225.69.23        UH         0         0   lan0:1      4136
10.225.69.0             10.225.69.21        U          3         0   lan0        1500
10.225.69.0             10.225.69.23        U          3         0   lan0:1      1500
127.0.0.0               127.0.0.1           U          0         0   lo0         4136
default                 10.225.69.21        U          0         0   lan0        1500
```

Appendix 22: Contents of /etc/passwd on stxhpcl1

```
root:/asrkIyd.U98c:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
nobody:*:-2:-2::/:
www:*:30:1::/:
oracle:fdOR4rxfx4GVs:101:101:,,,:/home/oracle:/usr/bin/ksh
oneworld:M9r.tGLRzhIWo:102:102:,,,:/home/oneworld:/usr/bin/ksh
owuser1:0q/e8hg5y5geo:103:102:,,,:/home/owuser1:/usr/bin/ksh
```

8318
4.

Appendix 23: Contents of /etc/passwd on stxhpcl2

```
root:8fdfhLf20HJWk:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
nobody:*:-2:-2::/:
www:*:30:1::/:
oracle:R6bu57ElPaWbk:101:101:,,,:/home/oracle:/usr/bin/ksh
oneworld:mkE94U1gpB6.k:102:102:,,,:/home/oneworld:/usr/bin/ksh
owuser1:HFi9CPzs0f0yw:103:102:,,,:/home/owuser1:/usr/bin/ksh
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 271
Doc. 3698

Appendix 24: Contents of /etc/services

```
# @(#)services $Revision: 1.32.214.7 $ $Date: 97/09/10 14:50:42 $
#
# This file associates official service names and aliases with
# the port number and protocol the services use.
#
# Some of the services represented below are not supported on HP-UX.
# They are provided solely as a reference.
#
# The form for each entry is:
# <official service name>  <port number/protocol name>  <aliases>
#
# See the services(4) manual page for more information.
# Note: The entries cannot be preceded by a blank space.
#
tcpmux          1/tcp                   # TCP port multiplexer (RFC 1078)
echo            7/tcp                   # Echo
echo            7/udp                   #
discard         9/tcp   sink null       # Discard
discard         9/udp   sink null       #
systat         11/tcp   users           # Active Users
daytime        13/tcp                   # Daytime
daytime        13/udp                   #
qotd           17/tcp   quote           # Quote of the Day
chargen        19/tcp   ttytst source   # Character Generator
chargen        19/udp   ttytst source   #
ftp-data       20/tcp                   # File Transfer Protocol (Data)
ftp            21/tcp                   # File Transfer Protocol (Control)
telnet         23/tcp                   # Virtual Terminal Protocol
smtp           25/tcp                   # Simple Mail Transfer Protocol
time           37/tcp   timeserver      # Time
time           37/udp   timeserver      #
rlp            39/udp   resource        # Resource Location Protocol
whois          43/tcp   nicname         # Who Is
domain         53/tcp   nameserver      # Domain Name Service
domain         53/udp   nameserver      #
bootps         67/udp                   # Bootstrap Protocol Server
bootpc         68/udp                   # Bootstrap Protocol Client
tftp           69/udp                   # Trivial File Transfer Protocol
rje            77/tcp   netrjs          # private RJE Service
finger         79/tcp                   # Finger
http           80/tcp   www             # World Wide Web HTTP
http           80/udp   www             # World Wide Web HTTP
link           87/tcp   ttylink         # private terminal link
supdup         95/tcp                   #
hostnames     101/tcp   hostname        # NIC Host Name Server
tsap          102/tcp iso_tsap iso-tsap # ISO TSAP (part of ISODE)
pop           109/tcp postoffice pop2 # Post Office Protocol - Version 2
pop3          110/tcp  pop-3           # Post Office Protocol - Version 3
portmap       111/tcp  sunrpc          # SUN Remote Procedure Call
portmap       111/udp  sunrpc          #
ident         113/tcp  authentication # RFC1413
sftp          115/tcp                  # Simple File Transfer Protocol
uucp-path     117/tcp                  # UUCP Path Service
nntp          119/tcp  readnews untp   # Network News Transfer Protocol
ntp           123/udp                  # Network Time Protocol
netbios_ns    137/tcp                  # NetBIOS Name Service
netbios_ns    137/udp                  #
netbios_dgm   138/tcp                  # NetBIOS Datagram Service
netbios_dgm   138/udp                  #
netbios_ssn   139/tcp                  # NetBIOS Session Service
netbios_ssn   139/udp                  #
bftp          152/tcp                  # Background File Transfer Protocol
snmp          161/udp  snmpd           # Simple Network Management Protocol Agent
snmp-trap     162/udp  trapd           # Simple Network Management Protocol Traps
bgp           179/tcp                  # Border Gateway Protocol
# PV performance tool services entries
pvserver      382/tcp    # PV server
```

8316
A.

```
pvalarm       383/tcp     # PV alarm management
#
# UNIX services
#
biff          512/udp  comsat          # mail notification
exec          512/tcp                 # remote execution, passwd required
login         513/tcp                 # remote login
who           513/udp  whod           # remote who and uptime
shell         514/tcp  cmd            # remote command, no passwd used
syslog        514/udp                 # remote system logging
printer       515/tcp  spooler        # remote print spooling
talk          517/udp                 # conversation
ntalk         518/udp                 # new talk, conversation
route         520/udp  router routed  # routing information protocol
efs           520/tcp                 # Extended file name server
timed         525/udp  timeserver     # remote clock synchronization
tempo         526/tcp  newdate        #
courier       530/tcp  rpc            #
conference    531/tcp  chat           #
netnews       532/tcp  readnews       #
netwall       533/udp                 # Emergency broadcasting
uucp          540/tcp  uucpd          # uucp daemon
remotefs      556/tcp  rfs_server rfs # Brunhoff remote filesystem
ingreslock   1524/tcp                 #
#
# Other HP-UX services
#
lansrm        570/udp                 # SRM/UX Server
DAServer      987/tcp                 # SQL distributed access
instl_boots  1067/udp                 # installation bootstrap protocol server
instl_bootc  1068/udp                 # installation bootstrap protocol client
nfsd-keepalive 1110/udp               # Client status info
nfsd-status    1110/tcp               # Cluster status info
msql         1111/tcp                 # Mini SQL database server
rlb          1260/tcp                 # remote loopback diagnostic
clvm-cfg     1476/tcp                 # HA LVM configuration
diagmond     1508/tcp                 # Diagnostic System Manager
nft          1536/tcp                 # NS network file transfer
sna-cs       1553/tcp                 # SNAplus client/server
sna-cs       1553/udp                 # SNAplus client/server
ncpm-pm      1591/udp                 # NCPM Policy Manager
ncpm-hip     1683/udp                 # NCPM Host Information Provider
cvmon        1686/udp                 # Clusterview cvmon-cvmap communication
registrar    1712/tcp                 # resource monitoring service
registrar    1712/udp                 # resource monitoring service
ncpm-ft      1744/udp                 # NCPM File Transfer
psmond       1788/tcp                 # Predictive Monitor
psmond       1788/udp                 # Hardware Predictive Monitor
pmlockd      1889/tcp                 # SynerVision locking daemon
pmlockd      1889/udp                 #
nfsd         2049/udp                 # NFS remote file system
netdist      2106/tcp                 # update(1m) network distribution service
rfa          4672/tcp                 # NS remote file access
veesm        4789/tcp                 # HP VEE service manager
hacl-hb      5300/tcp                 # High Availability (HA) Cluster heartbeat
hacl-gs      5301/tcp                 # HA Cluster General Services
hacl-cfg     5302/tcp                 # HA Cluster TCP configuration
hacl-cfg     5302/udp                 # HA Cluster UDP configuration
hacl-probe   5303/tcp                 # HA Cluster TCP probe
hacl-probe   5303/udp                 # HA Cluster UDP probe
hacl-local   5304/tcp                 # HA Cluster Commands
hacl-test    5305/tcp                 # HA Cluster Test
hacl-dlm     5408/tcp                 # HA Cluster distributed lock manager
lanmgrx.osB  5696/tcp                 # LAN Manager/X for B.00.00 OfficeShare
r4-sna-cs    5707/tcp                 # SNA client/server (up to Release 4.1)
SNAplus      5708/udp                 # SNA logical network A (up to Release 4.1)
r4-sna-ft    5709/tcp                 # SNA file transfer (up to Release 4.1)
hcserver     5710/tcp                 # HP Cooperative Services
grmd         5999/tcp                 # graphics resource manager
spc          6111/tcp                 # sub-process control
desmevt      6868/tcp                 # DE/. Services Monitor, Event Service
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 272
3698
Doc.

```
pdclientd    6874/tcp                # Palladium print client daemon
pdeventd     6875/tcp                # Palladium print event daemon
iasqlsvr     7489/tcp                # Information Access
recserv      7815/tcp                # SharedX Receiver Service
ftp-ftam     8868/tcp                # FTP->FTAM Gateway
mcsemon      9999/tcp                # MC/System Environment monitor
console      10000/tcp               # MC/System Environment console multiplexor
actcp        31766/tcp               # ACT Call Processing Server
#
# Kerberos (Project Athena/MIT) services
#
kerberos5     88/udp   kdc                 # Kerberos 5 kdc
klogin       543/tcp                 # Kerberos rlogin -kfall
kshell       544/tcp  krcmd          # Kerberos remote shell -kfall
ekshell      545/tcp  krcmd          # Kerberos encrypted remote shell -kfall
kerberos     750/udp  kdc            # Kerberos (server) udp -kfall
kerberos     750/tcp  kdc            # Kerberos (server) tcp -kfall
kerberos_master 751/tcp kadmin       # Kerberos kadmin
krbupdate    760/tcp  kreg           # Kerberos registration -kfall
kpasswd      761/tcp  kpwd           # Kerberos "passwd" -kfall
eklogin     2105/tcp                 # Kerberos encrypted rlogin -kfall
# The X10_LI server for each display listens on ports 5800 + display number.
# The X10_MI server for each display listens on ports 5900 + display number.
# The X11 server for each display listens on ports 6000 + display number.
# The X11 font server listens on port 7000.
# Do NOT associate other services with these ports.
# Refer to the X documentation for details.

hpoms-ci-lstn   5403/tcp      #SAP spooler support
hpoms-dps-lstn  5404/tcp      #SAP spooler support
samd            3275/tcp        # sam daemon

dtspc   6112/tcp       #subprocess control
```

Appendix 25: Output of <swlist>

```
# Initializing...
# Contacting target "stxhpcl1"...
#
# Target:  stxhpcl1:/
#

#
# Bundle(s):
#

  B3935BA       A.11.09         MC / Service Guard
  B3935DA       A.11.09         MC / Service Guard
  B5736BA       A.03.20         HA Monitors
  B5736DA       A.03.20         HA Monitors
  B7609BA       A.03.20         Event Monitoring Service
  HPUXEng32RT   B.11.00.01      English HP-UX 32-bit Runtime Environment
  UXCoreMedia   B.11.00.01      HP-UX Media Kit (Reference Only. See Description)
  XSWGR1100     B.11.00.47.08   General Release Patches, November 1999 (ACE)
```

8354
A.

Appendix 26: Contents of /stand/system

```
* Drivers and Subsystems

CentIf
CharDrv
DlkmDrv
GSCtoPCI
PCItoPCI
arp
asp
autofsc
beep
btlan3
c720
cb
ccio
cdfs
clone
core
diag0
diag2
dlkm
dlpi
dmem
echo
fc
fc_arp
fcgsc
fcgsc_lan
ffs
hpstreams
inet
ip
kload
klog
lan2
lasi
ldterm
lv
lvm
maclan
mux2
netdiag1
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 273
Doc: 3698

```
netqa
nfs_client
nfs_core
nfs_server
nfsm
nms
nuls
pa_generic_psm
pa_psm
pci
pckt
pipedev
pipemod
ps2
ptem
ptm
pts
rawip
sad
sc
sctl
sdisk
sio
stape
stcpmap
strlog
strpty_included
strtelnet_included
tcp
telm
tels
timod
tirdwr
tlclts
tlcots
tlcotsod
tun
udp
ufs
uipc
vxbase
wsio


* Kernel Device info

dump lvol


* Tunable parameters

STRMSGSZ        65535
bufpages        0
dbc_max_pct     20
maxfiles        2048
maxfiles_lim    2048
maxswapchunks   4096
maxuprc         ((NPROC*8)/10)
maxusers        400
maxvgs          80
msgmap          (MSGTQL+2)
msgmax          65535
msgmnb          65535
msgmni          (NPROC)
msgseg          32767
msgssz          128
msgtql          4096
nfile           (15*NPROC+2048)
nflocks         (NPROC)
ninode          (8*NPROC+2048)
nproc           (((10*MAXUSERS)/3)+128)
```

```
nstrpty          60
nstrtel          (MAXUSERS)
nswapdev         25
semmap           (SEMMNI+2)
semmni           (NPROC*2)
semmns           (SEMMNI*2)
semmnu           (NPROC-4)
semume           128
semvmx           32768
shmmax           0X40000000
shmmni           512
shmseg           32
swapmem_on       0
timeslice        1
unlockable_mem   (MAXUSERS*10)
```

8312
A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 274
Doc. 3698

Appendix 27: Output of <vgdisplay -v> on node stxhpcl1

```
--- Volume groups ---
VG Name                     /dev/vgcl1
VG Write Access             read/write
VG Status                   available, exclusive
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      4
Act PV                      4
Max PE per PV               1024
VGDA                        8
PE Size (Mbytes)            4
Total PE                    4092
Alloc PE                    4000
Free PE                     92
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/vgcl1/lv01
   LV Status                    available/syncd
   LV Size (Mbytes)             16000
   Current LE                   4000
   Allocated PE                 4000
   Used PV                      4


   --- Physical volumes ---
   PV Name                      /dev/dsk/c0t1d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t9d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t10d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t11d0
   PV Status                    available
   Total PE                     1023
   Free PE                      92
```

Appendix 28: Output of <vgdisplay -v> on node stxhpcl2

8310
A

```
--- Volume groups ---
VG Name                     /dev/vgcl2
VG Write Access             read/write
VG Status                   available, exclusive
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      4
Act PV                      4
Max PE per PV               1024
VGDA                        8
PE Size (Mbytes)            4
Total PE                    4092
Alloc PE                    4000
Free PE                     92
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/vgcl2/lv01
   LV Status                    available/syncd
   LV Size (Mbytes)             16000
   Current LE                   4000
   Allocated PE                 4000
   Used PV                      4


   --- Physical volumes ---
   PV Name                      /dev/dsk/c0t0d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t12d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t13d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t14d0
   PV Status                    available
   Total PE                     1023
   Free PE                      92
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 275
Doc. 3698

8309 A-

Appendix 29: OneWorld Xe IEO.ini file on node stxhpcl1

```
; RealTime initialization file INI(IEO)

[IEO]
RegisteredEvents=

[SAMPLE_EVENT]
DS1=DXXXXXXXX
DS2=DYYYYYYYY
DS3=DZZZZZZZZ
```

Appendix 30: OneWorld Xe IEO.ini file on node stxhpcl2

```
; RealTime initialization file INI(IEO)

[IEO]
RegisteredEvents=

[SAMPLE_EVENT]
DS1=DXXXXXXXX
DS2=DYYYYYYYY
DS3=DZZZZZZZZ
```

Appendix 31: OneWorld Xe JDE.ini file on node stxhpcl1

```
; OneWorld initialization file INI(JDE)
; HP9000 specific version - B73.3

[DEBUG]
Output=FILE
Trace=TRUE
ClientLog=1
DebugFile=/u03/oneworld/b733_sp14/log/jdedebug.log
JobFile=/u03/oneworld/b733_sp14/log/jde.log
LogErrors=1
JDETSFile=/u03/oneworld/b733_sp14/log/JDETS.log
RepTrace=0

[TAM]
TAMTraceLevel=0

[MEMORY DEBUG]
Frequency=10000
Full=1

[SVR]
EnvType=1
EnvironmentName=XDEVHPO2
SpecPath=spec
SourcePath=source
ObjectPath=obj
HeaderPath=include
HeaderVPath=includev
BinPath=bin32
LibPath=lib32
LibVPath=libv32
MakePath=make
WorkPath=work
CodeGeneratorPath=cg
ResourcePath=res
HelpPath=helps
NextIDPath=nextid
LibraryListName=XDEVHPO2

[INSTALL]
DefaultSystem=system
ClientPath=client
PackagePath=package
DataPath=data
B733=/u03/oneworld/b733_sp14
Double_Byte=0
LocalCodeSet=WE_ISO88591

[JDEIPC]
ipcTrace=0
maxNumberOfSemaphores=200
startIPCKeyValue=53000

[JDEMAIL]
Rule1=90|OPT|MAILSERVER=mail.jdedwards.com
Rule2=100|DEFAULT|OWMON=OWMON@jdedwards.com
Rule3=110|DEFAULT|JDE_SYSTEM=JDE_System@jdedwards.com
Rule4=120|DEFAULT|WORKFLOW_SYSTEM=Workflow@jdedwards.com
Rule5=130|OPT|MERGELOCAL=1
Rule6=140|OPT|UPDATELOCAL=0

[JDENET]
serviceNameListen=6005
serviceNameConnect=6005
maxNetProcesses=1
maxNetConnections=250
maxKernelProcesses=50
maxKernelRanges=20
```

8308
A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 276
Doc. 3698

```
netTrace=0
[JDENET_KERNEL_DEF1]
krnlName=JDENET RESERVED KERNEL
dispatchDLLName=libjdenet.sl
dispatchDLLFunction=JDENET_DispatchMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF2]
krnlName=UBE KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBEMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF3]
krnlName=REPLICATION KERNEL
dispatchDLLName=libjderepl.sl
dispatchDLLFunction=DispatchRepMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF4]
krnlName=SECURITY KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF5]
krnlName=LOCK MANAGER KERNEL
dispatchDLLName=libtransmon.sl
dispatchDLLFunction=TM_DispatchTransactionManager
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF6]
krnlName=CALL OBJECT KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchCallObjectMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=1

[JDENET_KERNEL_DEF7]
krnlName=JDBNET KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchJDBNETMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF8]
krnlName=PACKAGE INSTALL KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgInstallMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF9]
krnlName=SAW KERNEL
dispatchDLLName=libjdesaw.sl
dispatchDLLFunction=JDEK_DispatchSAWMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF10]
krnlName=SCHEDULER KERNEL
dispatchDLLName=libjdeschr.sl
dispatchDLLFunction=JDEK_DispatchScheduler
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0
```

```
[JDENET_KERNEL_DEF11]
krnlName=PACKAGE BUILD KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgBuildMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF12]
krnlName=UBE SUBSYSTEM KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBESBSMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF13]
krnlName=WORK FLOW KERNEL
dispatchDLLName=libworkflow.sl
dispatchDLLFunction=JDEK_DispatchWFServerProcess
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF19]
krnlName=EVN KERNEL
dispatchDLLName=libjdeie.sl
dispatchDLLFunction=JDEK_DispatchITMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF20]
krnlName=IEO KERNEL
dispatchDLLName=libjdeieo.sl
dispatchDLLFunction=JDEK_DispatchIEOMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[NETWORK QUEUE SETTINGS]
UBE Semaphore Key=3600
DefaultPrinterOUTQ=devprn6
JDENETTimeout=60

[BSFN BUILD]
BuildArea=/usr/oneworld/BDEV/b733/packages
OptimizationFlags=+O1
DebugFlags=-g -y -D_DEBUG -DJDEDEBUG
InliningFlags=
DefineFlags=-DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_HPUX_SOURCE
CompilerFlags=-Aa +w1 +z -c
OSReleaseLevel=+DAportable
LinkFlags=-b -z -B symbolic -L/usr/oneworld/BDEV/b733/system/lib -ljdesaw
LinkLibraries=
SimultaneousBuilds=0

[UBE]
UBEDebugLevel=0

[DB SYSTEM SETTINGS]
Version=43
Default User=JDESVR
Default Pwd=
Default Env=XDEVHPO2
Default PathCode=PROD
Base Datasource=ORACLE SVR
Object Owner=JDESVR
Server=corowsn1
Database=owsn1devl
Load Library=libora73.sl
Decimal Shift=Y
Julian Dates=Y
Use Owner=Y
Secured=Y
```

8306
A.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 277
Doc. 3698

```
Type=O
Library List=
TriggerLibrary=JDBTRIG

[LOCK MANAGER]
Server=hpcluster
AvailableService=TS
RequestedService=NONE

[SERVER ENVIRONMENT MAP]
ADEVASD1=ADEVHPO1
ADEVASD2=ADEVHPO2
ADEVNAO1=ADEVHPO1
ADEVNAO2=ADEVHPO2
ADEVNAS1=ADEVHPO1
ADEVNAS2=ADEVHPO2
ADEVNIS1=ADEVHPO1
ADEVNIS2=ADEVHPO2
ADEVRSO1=ADEVHPO1
ADEVRSO2=ADEVHPO2
ADEVCLA1=ADEVHPO1
ADEVCLA2=ADEVHPO2
PDEVASD1=PDEVHPO1
PDEVASD2=XDEVHPO2
PDEVNAO1=PDEVHPO1
PDEVNAO2=XDEVHPO2
PDEVNAS1=PDEVHPO1
PDEVNAS2=XDEVHPO2
PDEVNIS1=PDEVHPO1
PDEVNIS2=XDEVHPO2
PDEVRSO1=PDEVHPO1
PDEVRSO2=XDEVHPO2
PDEVCLA1=PDEVHPO1
PDEVCLA2=XDEVHPO2
PDEVHPO2=XDEVHPO2


[SECURITY]
User=JDESVR
Password=
DefaultEnvironment=XDEVHPO2
DataSource=ORACLE PVC B733
SecurityServer=hpcluster
ServerPswdFile=FALSE
History=0

[CLUSTER]
PrimaryNode=hpcluster

[JDEITDRV]
DrvCount=3
Drv1=Z:libzdrv.sl
Drv2=RT:librtdrv.sl
Drv3=JDENET:libjdetrdrv.sl

[Interoperability]
RealTimeEvents=*ALL
SaveDoc=0
```

Appendix 32: OneWorld Xe JDE.ini file on node stxhpcl2

```
; OneWorld initialization file INI(JDE)
; HP9000 specific version - B73.3

[DEBUG]
Output=FILE
Trace=TRUE
ClientLog=1
DebugFile=/u02/oneworld/b733_sp14/log/jdedebug.log
JobFile=/u02/oneworld/b733_sp14/log/jde.log
LogErrors=1
JDETSFile=/u02/oneworld/b733_sp14/log/JDETS.log
RepTrace=0

[TAM]
TAMTraceLevel=0

[MEMORY DEBUG]
Frequency=10000
Full=1

[SVR]
EnvType=1
EnvironmentName=XDEVHPO2
SpecPath=spec
SourcePath=source
ObjectPath=obj
HeaderPath=include
HeaderVPath=includev
BinPath=bin32
LibPath=lib32
LibVPath=libv32
MakePath=make
WorkPath=work
CodeGeneratorPath=cg
ResourcePath=res
HelpPath=helps
NextIDPath=nextid
LibraryListName=XDEVHPO2

[INSTALL]
DefaultSystem=system
ClientPath=client
PackagePath=package
DataPath=data
B733=/u02/oneworld/b733_sp14
Double_Byte=0
LocalCodeSet=WE_ISO88591

[JDEIPC]
ipcTrace=0
maxNumberOfSemaphores=200
startIPCKeyValue=33000

[JDEMAIL]
Rule1=90|OPT|MAILSERVER=mail.jdedwards.com
Rule2=100|DEFAULT|OWMON=OWMON@jdedwards.com
Rule3=110|DEFAULT|JDE_SYSTEM=JDE_System@jdedwards.com
Rule4=120|DEFAULT|WORKFLOW_SYSTEM=Workflow@jdedwards.com
Rule5=130|OPT|MERGELOCAL=1
Rule6=140|OPT|UPDATELOCAL=0

[JDENET]
serviceNameListen=6006
serviceNameConnect=6006
maxNetProcesses=1
maxNetConnections=250
maxKernelProcesses=50
maxKernelRanges=20
```


8304
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 278
Doc. 3698

8303
A.

```
netTrace=0

[JDENET_KERNEL_DEF1]
krnlName=JDENET RESERVED KERNEL
dispatchDLLName=libjdenet.sl
dispatchDLLFunction=JDENET_DispatchMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF2]
krnlName=UBE KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBEMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF3]
krnlName=REPLICATION KERNEL
dispatchDLLName=libjderepl.sl
dispatchDLLFunction=DispatchRepMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF4]
krnlName=SECURITY KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF5]
krnlName=LOCK MANAGER KERNEL
dispatchDLLName=libtransmon.sl
dispatchDLLFunction=TM_DispatchTransactionManager
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF6]
krnlName=CALL OBJECT KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchCallObjectMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=1

[JDENET_KERNEL_DEF7]
krnlName=JDBNET KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchJDBNETMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF8]
krnlName=PACKAGE INSTALL KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgInstallMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF9]
krnlName=SAW KERNEL
dispatchDLLName=libjdesaw.sl
dispatchDLLFunction=JDEK_DispatchSAWMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF10]
krnlName=SCHEDULER KERNEL
dispatchDLLName=libjdeschr.sl
dispatchDLLFunction=JDEK_DispatchScheduler
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0
```

```
[JDENET_KERNEL_DEF11]
krnlName=PACKAGE BUILD KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgBuildMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF12]
krnlName=UBE SUBSYSTEM KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBESBSMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF13]
krnlName=WORK FLOW KERNEL
dispatchDLLName=libworkflow.sl
dispatchDLLFunction=JDEK_DispatchWFServerProcess
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF19]
krnlName=EVN KERNEL
dispatchDLLName=libjdeie.sl
dispatchDLLFunction=JDEK_DispatchITMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF20]
krnlName=IEO KERNEL
dispatchDLLName=libjdeieo.sl
dispatchDLLFunction=JDEK_DispatchIEOMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[NETWORK QUEUE SETTINGS]
UBE Semaphore Key=3600
DefaultPrinterOUTQ=devprn6
JDENETTimeout=60

[BSFN BUILD]
BuildArea=/usr/oneworld/BDEV/b733/packages
OptimizationFlags=+O1
DebugFlags=-g -y -D_DEBUG -DJDEDEBUG
InliningFlags=
DefineFlags=-DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_HPUX_SOURCE
CompilerFlags=-Aa +w1 +z -c
OSReleaseLevel=+DAportable
LinkFlags=-b -z -B symbolic -L/usr/oneworld/BDEV/b733/system/lib -ljdesaw
LinkLibraries=
SimultaneousBuilds=0

[UBE]
UBEDebugLevel=0

[DB SYSTEM SETTINGS]
Version=43
Default User=JDESVR
Default Pwd=
Default Env=XDEVHPO2
Default PathCode=PROD
Base Datasource=ORACLE SVR
Object Owner=JDESVR
Server=corowsn1
Database=owsn1devl
Load Library=libora73.sl
Decimal Shift=Y
Julian Dates=Y
Use Owner=Y
Secured=Y
```

8302
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 2289
3698
Doc.

9303 A-

```
Type=O
Library List=
TriggerLibrary=JDBTRIG

[LOCK MANAGER]
Server=hpcluster2
AvailableService=TS
RequestedService=NONE

[SERVER ENVIRONMENT MAP]
ADEVASD1=ADEVHPO1
ADEVASD2=ADEVHPO2
ADEVNAO1=ADEVHPO1
ADEVNAO2=ADEVHPO2
ADEVNAS1=ADEVHPO1
ADEVNAS2=ADEVHPO2
ADEVNIS1=ADEVHPO1
ADEVNIS2=ADEVHPO2
ADEVRSO1=ADEVHPO1
ADEVRSO2=ADEVHPO2
ADEVCLA1=ADEVHPO1
ADEVCLA2=ADEVHPO2
PDEVASD1=PDEVHPO1
PDEVASD2=XDEVHPO2
PDEVNAO1=PDEVHPO1
PDEVNAO2=XDEVHPO2
PDEVNAS1=PDEVHPO1
PDEVNAS2=XDEVHPO2
PDEVNIS1=PDEVHPO1
PDEVNIS2=XDEVHPO2
PDEVRSO1=PDEVHPO1
PDEVRSO2=XDEVHPO2
PDEVCLA1=PDEVHPO1
PDEVCLA2=XDEVHPO2
PDEVHPO2=XDEVHPO2


[SECURITY]
User=JDESVR
Password=JDESVR
DefaultEnvironment=XDEVHPO2
DataSource=ORACLE PVC B733
SecurityServer=hpcluster2
ServerPswdFile=TRUE
History=0

[CLUSTER]
PrimaryNode=hpcluster2

[JDEITDRV]
DrvCount=3
Drv1=Z:libzdrv.sl
Drv2=RT:librtdrv.sl
Drv3=JDENET:libjdetrdrv.sl

[Interoperability]
RealTimeEvents=*ALL
SaveDoc=0
```

Appendix 33: HP's Partner Technology Access Center High Availability Implementation and Certification Services Data Sheet

Hewlett-Packard Company has a wide range of powerful high availability tools and services to assist ISVs in the certification of their applications in a highly available, mission-critical Hewlett-Packard environment.

8300
A.

HP's High Availability software tool suite, including MC/ServiceGuard, is a specialized facility for protecting mission-critical applications from hardware and software failures. With MC/ServiceGuard, multiple nodes (systems) are organized into an enterprise cluster that is capable of delivering highly available application services to LAN attached clients.

For ease of management and outstanding flexibility, MC/ServiceGuard allows all of the resources needed by an application to be organized into entities called "application packages". Application packages consist of any resource needed to support a specific application service, such as disks, network resources, and application or system processes. Packages are the entities that are managed and moved within the enterprise cluster.

When an ISV delivers an application that will be run in a mission critical environment, it is important to certify that the application has been configured and tested in an MC/ServiceGuard environment.

To aid ISVs in certifying their applications in a highly available environment, the HP Partner Technology Access Center (PTAC) provides hardware and consulting services. The following are the types of services provided:

- Analysis of Application Environment:
  - system resources used by the application
  - application design and number of packages
  - use of raw, HFS or JFS volumes
  - application recovery methods
  - data loss specifications
  - checkpointing or buffer flushing frequency
  - shared versus replicated file systems for code and/or data
  - use of memory-based data
  - capacity requirements
  - issues affecting failover time

- Cluster configuration of SCC hardware to match your application needs
- Define application packages and resources required
- Create application package control scripts:
  - application startup & shutdown
  - application monitoring
  - application error handling
  - application restart options
  - application IP addresses
  - service names
  - volume group handling
  - data recovery procedures

- Create, verify and execute a test plan which will exercise defined failure scenarios
- Demonstrate the functionality of the highly available cluster

The HP PTAC maintains the following hardware cluster, available for High Availability application certification:

- (2) L2000 2-way SMP processors
  - 4GB RAM per machine
  - 4 LAN interfaces per machine

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 280
3698
Doc.

- 360GB usable disk space

Additionally, the PTAC offers a High Availability Implementation and Verification Service for those ISVs who wish to verify their Windows NT applications with Microsoft Cluster Server.

Contact the Partner Technology Access Center for more information about these and additional services.

HP Partner Technology Access Center
W 120 Century Road
Paramus, NJ 07653
USA
Tel: (1) 516-753-3406

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

To aid Independent Software Vendors (ISVs) in certifying their applications in a highly available environment, the Hewlett-Packard (HP) Partner Technology Access Center (PTAC) provides hardware, HA training, and consulting services. The following are the types of services provided:

- Analysis of Application Environment
- Cluster configuration of PTAC hardware to match application needs
- Define application packages and resources required
- Create application package control scripts
- Create, verify and execute a test plan which will exercise defined failure scenarios
- Demonstrate the functionality of the highly available cluster

To perform this service, and to offer it as a repeatable deliverable, the PTAC has defined a process and methodology. The completion of this process will result in an ISVs application being certified by HP as being able to perform in a highly available environment.

An ISVs customer either:

- View the ISVs application as mission-critical
- Mandates that the application must be run in a highly available state

However, a typical ISV has limited experience with architecting and testing HA solutions. Additionally, hardware for failover testing is often unavailable.

Initial Activities

- Contact PTAC administration at 1/516-753-3406 and request the HA Certification Services Package.
- Read and share the package with your ISV.
- A knowledgeable engineer from the ISV must be present at the PTAC lab during the entire HA certification.
- If the ISV has an assigned HP TC, that TC may optionally be present for the HA certification.
- Call PTAC administration and schedule PTAC HA Lab time.

Homework

The HA Certification Services Package contains:

- MC/ServiceGuard (MC/SG) manual
- "Designing Highly Available Cluster Applications" white paper
- MS/SG product brief
- Example certification write-up
- Example cluster and package configuration scripts.

The goal of this step is that the ISV should understand HP's HA product family and understand how to architect his application for HA certification.

Planning

- What should the cluster look like during normal operations?
- What is the standard configuration of most customers?
- Can application modules be spread across multiple systems? Is this normal?
- Do all pieces of the application failover together to the failover machine?
- Can applications running on different machines failover to a shared failover machine?
- Is there any HA mechanism already built in to the app?
- What are the customers expectations of HP's HA product suite?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 281
Doc 3698

Technical Evaluation

- Evaluate the app per HA design rules
- Discuss each rule with the application engineers
- What does the app do today to handle a system panic or reboot?
- Does the app use any system specific calls (e.g. uname, gethostbyname, SPU_ID, etc.)?

The deliverable of this step is a write-up of any issues.

App Setup Without MC/SG

- Setup the system without MC/ServiceGuard
- Install the app on the primary system
- Install all shared data on separate external volume groups
- Use JFS file systems as appropriate
- Test the app on the primary system
- Perform a "standard" ISV-provided test to ensure the app is running correctly
- If possible, connect to the app through a client
- Crash the primary system, reboot it, and test how the app starts
- Document any manual procedures
- Can everything start from rc scripts?
- Write a script which brings up the app and all required services

The goal of this step is to ensure that the app can automatically be started and shutdown.

The deliverable of this step is the tasks or scripts which start the app automatically.

No MC/SG, 2 Systems

Try to failover the app to the failover system by hand:

- Connect the volume group to the second system, vgimport, create mount points, etc.
- Document what has to be created on the failover system for the certification whitepaper
- With the app NOT running on the primary system, try to bring it up on the failover system
- Repeat this process until the app will run on the failover system

The goal of this step is to ensure that the failover can occur manually.

Hands On with MC/SG

Configure the MC/SG Cluster:

- Cluster configuration
- Create package(s)
- Create package script
- Compile package configuration scripts and distribute
- Use these scripts as the "customer_defined" functions in the package control scripts

The deliverable of this step is the cluster and package scripts.

Testing

Testing should be performed with a client connected and under system load. This is to test how well and how quickly the application recovers from a failover when a large amount of "work" is queued.

- Halt the package on the primary system and move it to the failover system.
- Move the package back to the primary system.
- Fail one of the systems (e.g. power off, kill monitored process, LAN disconnect)
- Ensure that the package starts on the failover system
- Repeat failover from the failover system back to the primary

- Be sure to test all combinations of app load during testing
- Repeat the failover process under different application states (i.e. heavy user load, no user load, batch jobs, online transactions)
- Keep timing records of how long it takes to completely failover the app
- The customer of the ISV will want to know the failover timing as part of the certification process

8297
A.

Application Monitoring

- MC/SG can monitor the health of processes which are critical to the correct running of the app
- Or, a custom monitor script can be written to monitor specific ISV processes
- Monitor script can be written now, or be written at each customer site

Support and Write-up

- The ISV will own the MC/SG scripts, but the SCC will keep copies for our records
- Determine whether the ISV will want to come back to test new application releases
- HP supports MC/SG, and the ISV supports the concept of failover with its application

The PTAC HA engineer will work with the ISV to produce the following deliverables. A copy of these will be placed on the HP Advanced Technology Center (ATC) High Availability web page:

- Whitepaper with technical details of the failover, known issues and recommended configurations
- Package control script
- Package configuration file (ASCII)
- Press release on the integration

Example Timetable

To understand the progression of the HA certification process, here is a typical ISV certification scenario:

- Day 1: ISVs HP contact calls PTAC information line
- Day 2: HA Certification Services information package is e-mailed to HP contact
- Day 3: HP contact reviews documentation, and provides to ISV
- Day 4: ISV reviews documentation to understand what must be done prior to coming to the PTAC HA Lab
- Day 5: ISV reports to HP contact when they will be ready to begin certification process
- Day 5: HP contact schedules PTAC HA Lab and engineering time
- Day 6-10: ISV performs necessary homework in preparation for certification process. ISV gathers all non-HP-UX materials that will be needed for the certification. If so desired, ISV prepares a client machine for delivery to the PTAC HA Lab.
- Day 11: ISV travels to PTAC HA Lab in Paramus, NJ
- Day 12: ISV is given a half day of training on HPs HA product suite
- Day 12: ISV and PTAC engineer begin installation of ISV application on PTAC hardware
- Day 13-Day 17: ISV and PTAC engineer follow the HA certification process noted earlier in this document

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 282
3698
Doc.

8296
A

Notes:

- This is an example scenario. Timing and process progression will be different for each ISV.
- If the ISV wishes to test a client connection to his application, the ISV must supply the client machine. The PTAC lab will provide PC display monitors and PC keyboards.
- The ISV must provide all non-HP-UX material on 4mm DAT tape or CD-ROM. The PTAC HA Lab servers are on a private subnet, and cannot contact machines outside of the PTAC HA Lab.

For More Information...

To receive the PTAC HA Certification Services Package, leave your name and Telnet at 1/516-753-3406, along with the name of your ISV.

Once you have received and examined the PTAC HA Certification Services Package, you will want to schedule the PTAC lab, as well as a PTAC High Availability engineer. To do so, please leave your name, Telnet, ISV name and timeframe desired, on 1/516-753-3406.

Questions about this process and the PTAC HA Certification Service may be directed to:

Hewlett-Packard Company
Walt Saiko
Partner Technology Access Center
W 120 Century Road
Paramus, NJ 07653
USA
Tel: (1) 301-258-5974

Apêndice HO

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 283
3698
Doc.

Cisco Systems

8295
A.

Overview

CiscoWorks LAN Management Solution 2.2 Introduction

CiscoWorks LAN Management Solution (LMS) provides a robust set of applications for maintaining, monitoring, and troubleshooting a broad range of devices in an end-to-end Cisco AVVID (Architecture for Voice, Video and Integrated Data) network. Built upon popular Internet-based standards, CiscoWorks LMS enables network operators to more efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime from anywhere within the network. Taking advantage of a Web-based client/server architecture, CiscoWorks LMS can be easily integrated with other popular network management systems or other third-party management solutions running in the network.

CiscoWorks LMS provides a solid foundation of basic and advanced management applications that complement CiscoWorks products. Other CiscoWorks products include the CiscoWorks Routed WAN Management (RWAN) Solution, which addresses the needs of the WAN with response time and access list management. The IP Telephony Environment Monitor (ITEM) ensures the readiness and manageability of converged networks that support voice over IP (VoIP) and IP telephony traffic and applications. The Cisco VPN/Security Management Solution (VMS) provides an integrated set of Web applications with features that assist in the deployment and monitoring of virtual private network (VPN) and security devices. Together, CiscoWorks products offer leading-edge solutions for improving the accuracy and efficiency of your operations staff, increasing overall availability of your network through proactive planning and maximizing network security.

The Changing Campus LAN

A key part of the business infrastructure, today's LANs are critical systems. The management of local-area networks has evolved from being device centric, to now focusing on managing the convergence of both data and voice traffic over a common infrastructure. As a result, it has become increasingly important to isolate, troubleshoot, and monitor network devices so that connections and services are always available. CiscoWorks LMS delivers advanced discovery technologies, port assignment tools, sophisticated connectivity analysis, configuration management tools, and device and network diagnostic capabilities (including fault management and Remote Monitoring [RMON] traffic monitoring) to help manage the complexities of a converged network.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 284
Doc. 3698

8294
A

A Comprehensive Solution

CiscoWorks LMS combines applications and tools for configuring, monitoring, and troubleshooting the campus network. Designed to address the networks powered by Cisco today, it also provides a flexible framework to address the device management needs of networks converging voice, video, and data; networks being protected with Cisco SAFE Blueprint for network security technologies; and networks designed for content migration.

The CiscoWorks LMS consists of operationally focused tools. These tools include fault management, scalable topology views, sophisticated configuration, Layer 2/3 path analysis, voice-supported path trace, traffic monitoring, end-station tracking workflow application servers management, and device troubleshooting capabilities.

CiscoWorks LMS is built on the CiscoWorks common services foundation. This design facilitates operations workflow between applications by linking data collection, monitoring, and analysis tools—all from a single desktop application. For example, a user complaint of slow response time or a poor IP phone connection can be quickly diagnosed using CiscoWorks LMS Layer 2 path tools that automatically acquire user path information stored in one database, and highlight devices on a topology map. Additionally, switch or router configurations can then be quickly examined, or RMON traffic data can be reviewed to detect anomalies or the need for changes. Those actions may draw information from one or more applications.

CiscoWorks LMS uses Internet standards to tie together best-of-breed tools and to take advantage of their capabilities through data and task integration standards. Using the common information model (CIM) and Extensible Markup Language (XML), the industry standards for data-sharing CiscoWorks LMS offers a means of extracting data and using it with popular network management platform products. With the CiscoWorks LMS, Cisco offers a complete family of dedicated hardware Cisco Catalyst® network analysis modules (NAMs). Cisco Catalyst NAMs provide increased visibility into switched LAN environments comprising 10/100 and Gigabit Ethernet links for comprehensive, end-to-end, seven-layer monitoring of network infrastructures.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8293
A.

Solution Components

The following applications are included in CiscoWorks LMS:

- CiscoWorks Campus Manager—CiscoWorks Campus Manager is a suite of Web-based applications designed for managing networks powered by Cisco switches. These include Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, Layer2/3 path analysis tools, and IP phone user and path information.
- CiscoWorks Device Fault Manager—CiscoWorks Device Fault Manager provides real-time fault analysis for Cisco devices. It generates "intelligent Cisco traps" through a variety of data collection and analysis techniques. These can be locally displayed, e-mailed, or forwarded to other popular event management systems.
- nGenius Real-Time Monitor—The nGenius Real-Time Monitor is a Web-enabled multiuser traffic management tool set that provides access to network-wide, real-time RMON information for monitoring, troubleshooting, and maintaining network availability. Its applications graphically report and analyze device, link, and port level RMON collected traffic data from RMON-enabled Cisco Catalyst switches and internal network analysis module.
- CiscoWorks Resource Manager Essentials (RME)—CiscoWorks RME provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis.
- CiscoView—CiscoView is a Web-based tool that graphically provides real-time status of Cisco devices. The tool can drill down to display monitoring information on interfaces and access configuration functions.
- CiscoWorks Management Server—The CiscoWorks Management Server provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications.

Key Functions and Applications

Table 1 gives key functions and applications of the CiscoWorks LMS.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Offers intelligent, automatic discovery of Cisco devices to create topology views of the network	CiscoWorks Campus Manager	The Cisco Campus Manager Topology Services functionality discovers Cisco devices and calculates Layer 2 relationships to provide views of the Cisco network by ATM domain, VTP[1] domain, LAN edge view, and a general Layer 2 view.
Gives topology status indications	CiscoWorks Campus Manager	The topology maps indicate the discovery and SNMP[2] status of Cisco devices; these maps also are launching points for other CiscoWorks applications.
Configures, manages, and monitors VLAN[3] and ATM services/networks	CiscoWorks Campus Manager	CiscoWorks Campus Manager provides tools for creating, deleting, and editing VLANs; it provides ATM tools for displaying virtual circuits and for configuring SPVCs/SPVPs.[4]

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
285
Fls. Nº
3698
Doc.

8292
A.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Discovers end stations and IP phones connected to switch ports and identifies user locations based on user ID	CiscoWorks Campus Manager	The CiscoWorks Campus Manager User Tracking functionality correlates MAC[5] address and IP address to switch port; integration with Microsoft's PDC and Novell's NDS tree provides the user ID for even more efficient user location and tracking.
Traces Layer 2 and Layer 3 connectivity between two points (devices, servers, phones) in the network	CiscoWorks Campus Manager	The CiscoWorks Campus Manager Path Analysis tool performs path analysis for Layer 2 and Layer 3 devices using the device host name or IP address, and shows results on a map display, in a table display, or in a trace display.
Intelligently analyzes fault conditions designed to detect problems before they become network disruptions	CiscoWorks Device Fault Manager	CiscoWorks Device Fault Manager automated fault detection recognizes common problems in networks without forcing users to define their own rules sets, SNMP trap filters, or device polling intervals.
Interprets fault conditions at both the device and VLAN levels	CiscoWorks Device Fault Manager	With the characteristics of over a 100 Cisco routers and switches predefined, new device support is easily added via Cisco.com. Cisco Device Fault Manager simplifies managing both Layer 2 and Layer 3 environments.
Collects RMON/RMON2 statistics from LAN switches, NAMs, and legacy Cisco SwitchProbe® devices	nGenius Real-Time Monitor	nGenius Real-Time Monitor monitors LAN traffic for protocols, applications, and interfaces to apply appropriate filters, reducing costs and increasing performance.
Provides for LAN troubleshooting at network and application packet levels	nGenius Real-Time Monitor	nGenius Real-Time Monitor helps resolve network and application issues by providing total network visibility from the application layer down to the data link layer for virtually any topology that exists today.
Offers detailed software and hardware inventory reporting	Cisco RME	Cisco RME provides accurate Cisco inventory baseline information, including memory, slots, software versions, and boot ROMs needed to make decisions about the network.
Offers automated update engines for device software and configuration changes	Cisco RME	Cisco RME allows software and configuration updates to be sent to selected devices on a scheduled basis; it reduces time and errors involved in network updates.
Offers a consolidated troubleshooting tools device center	Cisco RME	A wide collection of switch and router analysis tools is accessible from a single location; third-party applications can link to the device center.
Offers centralized change audit logging	Cisco RME	A comprehensive change-monitoring log records users and applications that are active on the network.
Offers graphical device management	CiscoView	CiscoView displays a browser representation of Cisco router and switch devices, color-coded to indicate operational states, with access to configuration and monitoring tools.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8291
A.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Provides application access security	CiscoWorks Server	The CiscoWorks desktop controls user access to applications, ensuring that only appropriate classes of users can access tools that change network parameters versus read-only tools.
Offers third-party integration tools (Integration utility)	CiscoWorks Management Server	The CiscoWorks Management Server simplifies the Web integration of third-party and other Cisco management tools.

1. Virtual Trunking Protocol
2. Simple Network Management Protocol
3. Virtual LAN
4. Soft permanent virtual circuits/soft permanent virtual paths
5. Media Access Control

Key Functions and Applications

Deployment Options

Consider the following when installing the CiscoWorks LAN Management Solution:

- All applications do not have to be installed initially; applications not installed initially may be installed later.
- Most applications require the CiscoWorks Management Server from the Common Services CD (formerly CD One), which must be installed first.
- The CiscoWorks Campus Manager application depends on CiscoWorks RME, which is included as part of the CiscoWorks LAN Management Solution.

All solutions can coexist on the same server if they support and operate with the services of Common Services 2.2. However, network managers may want to consider such factors as the number of applications hosted, system resources, and number of devices to be managed in determining if all or a subset of the solutions are installed on the same server.

CiscoWorks solutions offer deployment flexibility. System administrators should use the guidelines given previously when planning the deployment of the various solution bundles. Some components within a solution require the CiscoWorks Management Server and must be installed on that machine. CiscoView and nGenius Real Time Monitor software can be set up on an independent server. The placement of components is a function of performance requirements and the size of the network.

Server System Requirements

Hardware/Operating System

UNIX

- System: Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) running Solaris 2.8 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM for workstations, 2-GB RAM for servers, 8-MB e-cache

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 286
3698
Doc.

8280
A

- Available disk: 40-GB internal FC-AL disk drive for workstation and dual drives of this type for server configurations

Windows

- System: IBM PC compatible with 550-MHz or higher Pentium III processor running Microsoft Windows 2000 Advanced Server (with Terminal Services turned off), Server or Professional Edition with Service Pack 2 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM
- Available disk: 40 GB with 2-GB swap recommended

Note: These system requirements are based on managing 500 devices with CiscoWorks RWAN and LAN Management solutions loaded on a single server. Refer to the Installation documentation for more information on required operating system patches.

Client Browser System Requirements

Hardware/Operating System

UNIX

- System: Sun Ultra 10 running Solaris Version 2.7 or 2.8
- System: HP9000 Series running HP-UX 11.0
- System: IBM RS/6000 workstation running AIX 4.3.3
- Memory: 256 MB

Windows

- System: IBM PC-compatible computer with 300-MHz or higher Pentium processor running Windows XP Professional, Windows 2000 (Advanced Server, Server or Professional) with Service Pack 3
- Memory: 256 MB

Note: Refer to the installation documentation for more information on required operating system patches.

Web Browser

UNIX

- Solaris: Netscape v4.76
- HP-UX: Netscape v4.78, 4.79
- AIX: Netscape v4.78, 4.79

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Windows

- Windows 2000/XP: Netscape v4.78, 4.79
- Windows 2000/XP: Internet Explorer v6.0.26

Note: Refer to the Installation documentation for more information on required operating systems patches, browser plug-ins, or Java Virtual Machine (JVM) versions.

Service and Support

CiscoWorks products are covered by the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 7 x 24 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A Cisco SAS contract ensures that customers have easy access to the information and services needed to stay up-to-date with newly supported device packages, patches, and minor updates. For further information on service and support offerings, contact your local sales office.

Ordering Information

8289

A.

The CiscoWorks LAN Management Solution includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris Workstation/Server. The products within this solution can be combined with other CiscoWorks products if they support the same CiscoWorks Management Server version, operating environment, and system requirements. Contact your local Cisco representative for available white papers and documentation outlining best practices for implementing a CiscoWorks management solution architecture.

To place an order, contact your Cisco sales representative.

Refer to the CiscoWorks LAN Management Solution individual product data sheets for more information on operating environment and system requirements.

For More Information

For more information on the CiscoWorks LAN Management Solution, visit http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2425/index.html.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

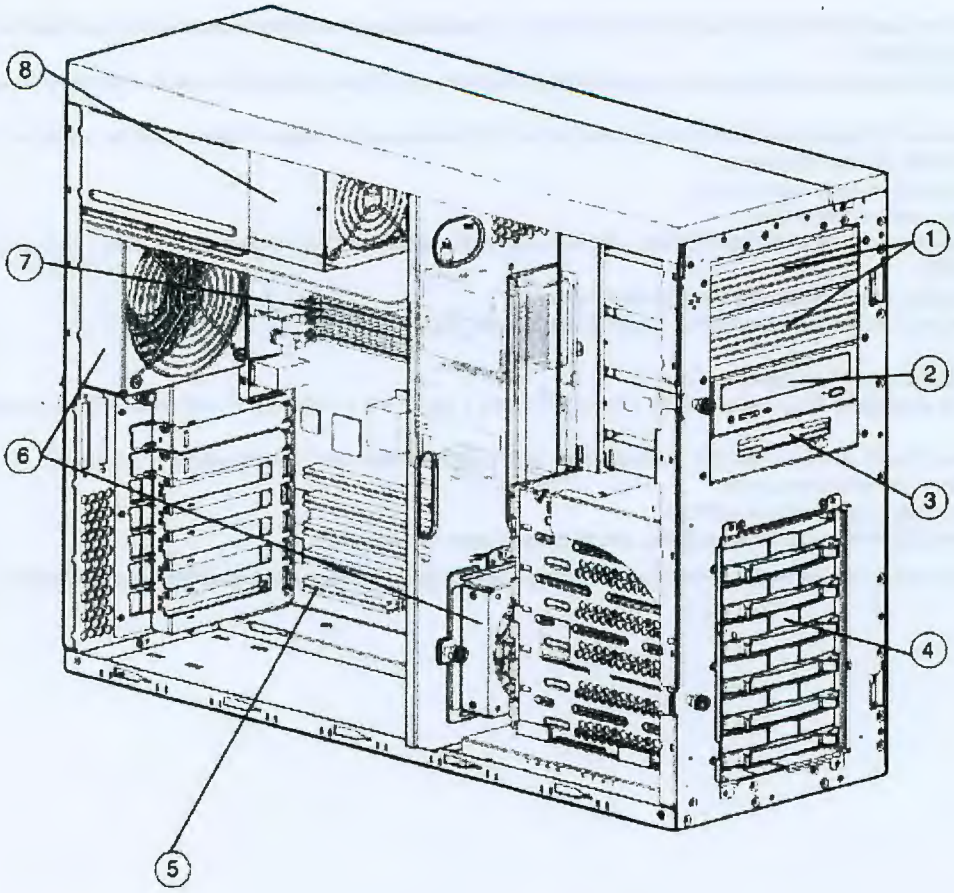
All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203046/ETMC 08.03

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 287
3698
Doc.

RQS nº 03/2005 - C
CPMI - CORREIOS
Fls. Nº 288
Doc. 3698

Overview



1. Two Removable Media Bays
2. 48X Max IDE (ATAPI) CD-ROM Drive
3. 1.44 Floppy Drive
4. Six 1" Hot Plug Drive Bays
5. Five expansion slots(four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI)
6. System fan
7. DIMM sockets for up to 8GB of memory, optionally interleaved
8. Optional 2nd Power Supply for hot-pluggable 1+1 redundancy

What's New

- Now available with Intel®Xeon 2.8 GHz Processors with 533MHz system bus.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 289
Doc.

Overview

8287 A.

At A Glance

- The ProLiant ML350 G3 is an expandable rack or tower platform delivering affordable 2-way performance and essential availability to corporate workgroups and growing businesses
- Intel Xeon 2.4 GHz or 2.8 GHz processors (dual processor capability) with 512-KB level 2 cache standard (full speed) and Hyper-Threading Technology
- ServerWorks Grand Champion LE Chipset with 533-MHz Front Side Bus for 2.8GHz processor models or 400-MHz FSB for models < 2.8 GHz
- Integrated Dual Channel Wide Ultra3 SCSI Adapter
- Smart Array Controller (standard in Array Models only)
- NC7760 PCI Gigabit Server Adapter (embedded)
- 512MB of 2-way interleaving capable PC2100 DDR SDRAM, with Advanced ECC capabilities (Array models only; 256MB standard on other models): Expandable to 8GB
- Flexible memory configurations allow interleaving (2x1) or non-interleaving
- Five available expansion slots: four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI
- Two USB ports
- Standard 6 x 1" Wide Ultra320 ready Hot Plug Drive Cage
- Internal storage capacity of up to 880GB (6 x 146.8 GB 1"), 1.174-TB (2 x 146.8 GB 1" + 6 x 146.8 GB 1") with optional 2-bay hot plug drive cage option
- 500W Hot-Pluggable Power Supply (standard) and an optional 500W Hot-Pluggable Redundant Power Supply (1 + 1) available
- Tool-free entry to chassis and access to components
- RBSU (ROM based setup utility) support, redundant ROM
- Insight Manager, SmartStart, ROM-based BIOS Setup Utility, and Automatic Server Recovery (ASR-2)
- Protected by HP Services, including a three-year, next business day, on-site, limited global warranty and extended Pre-Failure Warranty.

8286

A.

Standard Features

Processor *One of the following depending on Model:*	Intel Xeon Processor 2.8 GHz/533-512KB Intel Xeon Processor 2.4 GHz/400-512KB
Cache Memory	Integrated 512-KB Level 2 cache (full speed)
Upgradability	Upgradable to dual processing
Chipset	ServerWorks Grand Champion LE Chipset with 400-MHz or 533-MHz Front Side Bus (model dependent) NOTE: For more information regarding ServerWorks, please see the following URL: http://www.serverworks.com/products/overview.html NOTE: This Web site is available in English only.
Memory (One of the following depending on model)	2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities Standard (Non-Array Models) 256MB Standard (Array Models) 512MB Maximum 8 GB
Network Controller	NC7760 Gigabit Server Adapter (embedded)
Expansion Slots	I/O (5 Total, 5 Available) 64-bit/100MHz, PCI — 4 (4 available) (Array model has 3 available) — PCI Voltage: 3.3 Volt or universal cards 32-bit/33MHz, PCI — 1 (1 available) — 5 Volt or universal cards
Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 641 Controller (2.8 GHz Array Models Only)
Storage	Diskette Drives: 1.44 MB CD-ROM: 48x IDE (ATAPI) CD-ROM Drive Hard Drives: None Maximum Internal Storage: 1.174 TB GB (6 x 146.8 GB 1" with standard internal hot plug drive cage + (2 x 146.8 GB 1") with optional ML3xx Two Bay Hot Plug SCSI Drive Cage) External Storage: Two external SCSI knockouts available, optional ProLiant ML350 Internal to External SCSI Cable Option Kit required • HD68 Internal to External SCSI Cable Option Kit PN 159547-B22 • VHDCI Internal to External SCSI Cable Option Kit PN 333370-B21

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 290
Page 3
3698
Doc.

Standard Features

8285 A

Interfaces	Parallel	1
	Serial	1
	Pointing Device (Mouse)	1
	Graphics	1
	Keyboard	1
	Network RJ-45	1
	USB	2 NOTE: Please see the following URL for additional information regarding USB support: http://www.compaq.com/products/servers/platforms/usb-support.html. NOTE: This Web site is available in English only.
	External SCSI knockouts	2

Graphics	Integrated ATI RAGE XL Video Controller with 8-MB SDRAM Video Memory

Form Factor	Tower or rack (5U) NOTE: Rack models (and rack conversion kit) support: • Square hole racks from 27"- 32" deep (including Compaq/HP 7000, 9000, 10000 and H9 series) • Square or round hole racks, from 24" - 35" deep (including HP Rack System /E and HP Systems, with an adjustment) • Telco racks with 3rd part option kit from Rack Solutions http://www.racksolutions.com/compaq/products.htm NOTE: This Web site is available in English only.

Standard Features

8284
A.

ProLiant Essentials Foundation Pack Software	Insight Manager 7	Insight Manager 7 helps maximize system uptime and performance and reduces the cost of maintaining the IT infrastructure by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. Insight Manager 7 is easy to set up and provides rapid access to detailed fault and performance information gathered by the Management Agents. One-click-access to the Remote Insight Lights Out Edition II board allows systems administrators to take full graphical control of ProLiant servers in remote locations or lights-out data centers. Finally, Insight Manager 7 in concert with the Version Control Agents and Version Control Repository Manager enables systems administrotors to version manage and updote system software across groups of ProLiant servers.
	Management Agents	The Management Agents form the foundation for HP's Intelligent Manageability strategy. They provide direct, browser-based access to in-depth instrumentation built into HP servers, workstations, desktops, and portables, and send alerts to Insight Monager 7 and other enterprise management applications in case of subsystem or environmental failures. For additional information about the Management Agents ond other monagement products from HP, please visit the management Web site at http://www.hp.com/servers/manage.
	SmartStart	SmartStart is a tool that simplifies server setup, providing a rapid way to deploy reliable and consistent server configurations. For more information, please visit the SmartStart website at http://www.hp.com/servers/manage. SmartStart versian supported (minimum): SmartStart 5.50
	ActiveUpdate	ActiveUpdate is a web-based application that keeps IT managers directly connected to HP for prooctive notification and delivery of the latest software updates.
	ROMPaq, support software, and configuration utilities	The latest software, drivers, and firmware fully optimized and tested for your ProLiant server and options.
	Survey Utility and diagnostics utilities	The most advanced configuration analysis, reporting and troubleshooting utilities used by HP and ot your fingertips.
	Optional Proliant Essentials Value Packs	Optional software offerings that selectively extend the functionality of an Adaptive Infrastructure to address specific business problems and needs: • Rapid Deployment Pack – an automated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to chonging business demands. • Workload Management Pack – provides easier management of complex environments, improving overall server utilization and enabling Windows 2000 customers for the first time to confidently deploy multiple applications on a single multiprocessor ProLiant Server. • Performance Management Pack – o performance management solution that identifies and explains hardware performance bottlenecks on ProLiant servers and attached options enabling users to better utilize their valuable resources.

NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Volue Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more informotion.
NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials
NOTE: These Web sites are available in English only.

Industry Standard Compliance	ACPI V1.0B Compliant PCI 2.2 Compliant PXE Support WOL Support PCI-X 1.0 Compliant Novell Certified Microsoft Logo certifications

RQS nº 03/2005 - CN
CPMI - CORREIOS
291
Fls Nº
3698
Doc.

Standard Features

Manageability	Insight Manager 7 Redundant ROM System Firmware Update ROMPaq Remote Insight Lights-Out Edition II (optional) ProLiant RBSU (ROM-Based Setup Utility) Automatic Server Recovery-2 (ASR-2) Drive Parameter Tracking (with Smart Array Controller) Dynamic Sector Repairing (with Smart Array Controller) Pre-Failure Warranty (covers processors, memory and hard drives)
Security	Power-on password Setup password Diskette boot control Parallel and serial interface control Disk configuration lock Power switch security
Server Power Cords	One Lowline NEMA pawer cord and one Highline IEC Power cord ship standard Tower models ship with standard country specific power cords. Rack models ship with IEC cables. Depending on the country, some also ship with country specific power cords Redundant power supply options ship with country specific power cords with the exception of the -B21 Rack SKU which ships with an IEC cable only.
Power Supply	500 Watts, Power Factor Correction (PFC), Hot Plug 100 to 240 VAC Rated Input Voltage (Auto-sensing), CE Mark Compliant Optional 2nd Power Supply for hot-pluggable 1 + 1 redundancy.
System Fans	2 fans ship standard, 2 fans total supported (does not include power supply fans)
Required Cabling	For required cabling information, refer to the HP Web site at http://www.hp.com/servers/proliantML350. NOTE: This Web site is available in English only.
OS Support	Microsoft Windows NT® Server 4.0 and Terminal Server 4.0 Microsoft BackOffice Small Business Server 2000 Microsoft Windows 2000 Server and Advanced Server Windows Server 2003 Novell NetWare 5.1, 6.0 Novell NetWare Small Business Suite 6.0 SCO OpenServer 5.0.6a SCO OpenUnix 8 SCO UnixWare 7.1.1 IBM OS/2 Warp Server for e-business LINUX (Red Hat, 2.1 Advanced Server, Red Hat 8.0 and Red Hat 7.3, SuSE, SLES7, UnitedLinux 1.0) NOTE: For a more complete and up-to-date listing of supported OSs and versions, please visit our OS Support Matrix at: ftp://ftp.compaq.com/pub/products/servers/os-support-matrix-310.pdf NOTE: Optionol hordware may be required to support some operating systems. NOTE: For an up-to-date listing of the latest drivers available for the ProLiant ML350, please see: http://www.compaq.com/support/files/server/us/index.html. NOTE: These Web sites are available in English only.

Standard Features

8282
A.

Rack Airflow Requirements

- Rack 9000 and 10000 series Cabinets
  The increasing power of new high-performance processor technology requires increased cooling efficiency for rack-mounted servers. The 9000 and 10000 Series Racks provide enhanced airflow for maximum cooling, allowing these racks to be fully loaded with servers using the latest processors.

- Rack 7000 series Cabinets
  When installing a server with processors running at speeds of 550 MHz or greater in Rack 7000 series racks with glass doors (165753-001 (42U), and 163747-001 (22U)), the new processor technology requires the installation of HP's new High Airflow Rack Door Inserts (327281-B21 (42U), 327281-B22 (42U 6 pack), or 157847-B21 (22U)) to promote enhanced airflow for maximum cooling.

CAUTION: If a third-party rack is used, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment:

- Front and rear doors: If your 42U server rack includes closing front and rear doors, you must allow 830 square inches (5,350 sq cm) of hole evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).
- Side: The clearance between the installed rack component and the side panels of the rack must be a minimum of 2.75 inches (7 cm).

CAUTION: Always use blanking panels to fill all remaining empty front panel U-spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

NOTE: For additional information, refer to the Setup and Installation Guide or the Documentation CD provided with the server, or to the server documentation located in the Support section at the following URL:
http://www5.hp.com/servers/proliantml350
NOTE: This Web site is available in English only.

Installation of Server into Telco Racks

ML350 G3 rack model support: Support for all 2-post Telco racks requires the use of the rack kit and an additional option kit from Rack Solutions. http://www.racksolutions.com/compaq
NOTE: This Web site is available in English only.

HP Factory Express Capabilities

HP Factory Express gives you the flexibility to choose from a full menu of factory capabilities all in one manufacturing facility, in one process, with one touch giving you full control and access to HP's World class manufacturing facility anytime. This approach provides you the speed to deploy your IT needs, with total quality assurance, reliability, and predictability to lower your total cost of ownership by letting HP install, rack, and customize your software and hardware options for you.

RQS nº 03/2005 - CN
CPMI - CORREIOS
292
Fls. Nº Page 7
Doc. 3698

Standard Features

8285 A.

Service and Support

HP Services provides a three-year, limited warranty, including Pre-Failure Warranty (coverage of hard drives, memory and processors) fully supported by a worldwide network of resellers and service providers and lifetime toll-free 7 x 24 hardware technical phone support. In addition, available service offerings include:
NOTE: Limited Warranty includes 3 year Parts, 3 year Labor, 3-year on-site support.

A full range of HP Care Pack packaged hardware and software services:

- Installation and start up
- Extended coverage hours and enhanced response times
- System management and performance services
- Availability and recovery services

NOTE: For more infomation, visit http://www.hp.com/services/carepack.

Please see the following URL regarding Warranty Information For Your HP Products:
http://www.compaq.com/support/warranty_upgrades/web_statements/176738.html.

For additional information regarding Worldwide Limited Warranty and Technical Support, please see the following URL:
ftp://ftp.compaq.com/pub/supportinformation/ejourney/176738.pdf.
NOTE: These Web sites are available in English only.

NOTE: Certain restrictions and exclusions apply. Consult the Customer Support Center at 1-800-345-1518 for details.

Models

8280
A.

ML350T03 X2.8-512KB/533, 256MB *311523-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.8-512KB/533, 256MB *311524-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)
ML350T03 X2.8-512KB/533, 512MB Array *311525-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML[illegible]R03 X2.8-512KB/533, 512MB Array *311526-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB of Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 293
Doc. 3698

Models

ML350T03 X2:4-512KB/400, 256MB *269786-001*	Processor(s)	(1) Intel Xeon Processor 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hord Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)

ML350R03 X2.4-512KB/400, 256MB *269787-001*	Processor(s)	(1) Xeon 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drives & drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Options

8278
A.

ProLiant ML350 G3 Unique Options	Hot Plug Redundant Power Supply Option Kit	283655-001
	Hot Plug Redundant Power Supply Option Kit (cable) NOTE: PN 283655-B21 SKU contains the 2nd power supply with an IEC power cable. Only purchase if connecting to PDU/UPS thot supports IEC cables. All other SKUs contain country specific power cables.	283655-B21
	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as those with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 257913-B21) supports the ProLiant ML350 G3 servers.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283702-B21) supports the ProLiant ML350 G3 servers.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283701-B21) supports the ProLiant ML350 G3 servers.	283701-B21
	ProLiant ML350 G3 Tower to Rack Conversion Kit (CPQ brand)	290683-B21
ProLiant Essentials Value Pack Software	Rapid Deployment Pack, 1 User, V1.x NOTE: This license allows 1 server to be managed and deployed via the Deployment Server.	267196-B21
	Rapid Deployment Pack, 10 Users, V1.x NOTE: This license allows 10 servers to be managed and deployed via the Deployment Server.	269817-B21
	Flexible Quantity License Kit	302127-B21
	License-Only - for use with a Master License Agreement	302128-B21
	ProLiant Essentials Workload Management Pack 2.0 (Featuring Compaq Resource Partitioning Manager version 2.0)	303284-B21
	ProLiant Essentials Performance Management Pack Flexible License NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentiols or the various ProLiant Essentials Value Pack product QuickSpecs for more information. NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials. NOTE: These Web sites are available in English only.	306697-B21
HP NetServer Transition Services	HP NetServer to ProLiant integration and assessment service NOTE: HP identifies current levels of NetServer support, services, and management. This service helps maximize customer's ability to add ProLiant platforms into their current environment.	304164-002
	HP TopTools to Insight Manager 7 installation and startup service NOTE: Provides on-site review, installation and configuration services for Insight Manager 7. HP will also re-create, as closely as possible, the views and reports from the customer's current TopTools configuration. This service assures a smooth transition to the ProLiant Essentials software.	304163-002
	HP NetServer to ProLiant Essentials Rapid Deployment Pack installation and startup service NOTE: Install and configure Rapid Deployment Pack in a test environment, then deploy a server image to a maximum of 250 systems in the production environment. This service helps to assure successful system deployment.	304162-002

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 294
Doc. 3691

Options
8211
A

Processors	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such os thhose with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 257913-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283702-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283701-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	283701-B21
Memory (DIMMs)	NOTE: The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship stondord with one 256MB DIMM or one 512MB DIMM (Array models). For best performance automatically invoke interleaving by populating memory in identical pairs. If 1GB of total memory is desired add three 256MB DIMMs to the base configuration. If 1.5GB of memory is desired add one 256MB DIMM (to pair with the standard DIMM) and two 512MB DIMMs. Interleaving and installation of memory in pairs is not required. Add any combination of memory DIMMs below to operate in non-interleaved mode. NOTE: Each SDRAM Memory kit contains one (1) DIMM.	
	128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
	256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
	512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
	1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
	2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21
Internal Storage	ML3xx Two Bay Hot Plug SCSI Drive Cage NOTE: The drive cage option kit (PN 244059-B21) has one 1" drive bay and one 1.6" drive bay. It installs in two available removable media bays.	244059-B21
Optical Drives	16X DVD-ROM Drive Option Kit (Carbon)	217053-B21
	CD-RW/DVD-ROM 48X Combo Drive Option Kit	331346-B21
Hard Drives	*Ultra320 – Universal Hot Plug*	
	146.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286716-B22
	72.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286714-B22
	36.4-GB 10,000 rpm U320 Universal Hard Drive (1")	286713-B22
	72.8-GB 15,000 rpm U320 Universal Hard Drive (1")	286778-B22
	36.4-GB 15,000 rpm U320 Universal Hard Drive (1")	286776-B22
	18.2-GB 15,000 rpm U320 Universal Hard Drive (1")	286775-B22
	NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates. NOTE: Please see the Wide Ultra320 Universal Hot Plug QuickSpecs for additional technical information on the hard drives Support details, please see the following: http://www5.compaq.com/products/quickspecs/11531_na/11531_na.HTML	

Options

Storage Controllers	Smart Array 6402/128 Controller	273915-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Compaq RAID LC2 Controller	188044-B21
	Smart Array 532 Controller	225338-B21
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Ultra3 Channel Expansion Module for Smart Array 5300 Controller	153507-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-B21
	RAID ADG Upgrade for Smart Array 5302	288601-B21
	256-MB Battery Backed Cache Module NOTE: This 256-MB Battery Backed Cache Module supports the Smart Array 5300 series controllers, MSA 1000 and the Smart Array Cluster Storage.	254786-B21
	256MB Cache Upgrade for SA-6402 NOTE: This 256-MB Battery-Backed Cache Module upgrade kit supports the Smart Array 6400 series controller only.	273913-B21
	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS	284688-B21
	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter	268351-B21
	NOTE: Please see the following Controller or SCSI Adapter QuickSpecs for Technical Specifications such as PCI Bus, PCI Peak Data Transfer Rate, SCSI Protocols supported, SCSI Peak Data Transfer Rate, Channels, SCSI Ports, Drives supported, Cache, RAID support, and additional information: http://www5.compaq.com/products/quickspecs/10652_na/10652_na.HTML (RAID LC2) http://www5.compaq.com/products/quickspecs/10851_na/10851_na.HTML (Smart Array 532) http://www5.compaq.com/products/quickspecs/10640_na/10640_na.HTML (Smart Array 5300 Series) http://www5.compaq.com/products/quickspecs/11328_na/11328_na.HTML (Smart Array 5312) http://www5.compaq.com/products/quickspecs/11587_na/11587_na.HTML (Smart Array 6402) http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML (Smart Array 641) http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML (Smart Array 642) http://www5.compaq.com/products/quickspecs/10429_na/10429_na.HTML (SCSI Adapter) http://www5.compaq.com/products/quickspecs/11555_nav/11555_na.HTML (U320 Adapter)	
Wireless HAP Solution	Compaq WL410 Wireless SMB Access Point	191811-001

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Options

Communications	NC3123 Fast Ethernet NIC PCI 10/100 WOL and PXE	174830-B21
	NC3134 Fast Ethernet NIC 64 PCI Dual Port 10/100	138603-B21
	NC3135 Fast Ethernet Module Dual 10/100 Upgrade Module for NC3134	138604-B21
	NC6132 1000 SX Upgrade Module for NC3134	338456-B23
	NC6136 Gigabit Server Adapter, 64-bit/66MHz, PCI, 1000 SX	203539-B21
	NC6170 Dual Port PCI-X 1000SX Gigabit Server Adapter	313879-B21
	NC6770 PCI-X Gigabit Server Adapter, 1000-SX	244949-B21
	NC7170 Dual Port PCI-X 1000T Gigabit Server Adapter	313881-B21
	NC7132 Gigabit Upgrade Module 10/100/1000-T	153543-B21
	NC7770 PCI-X Gigabit server adapter	244948-B21
	56K v.90 PCI Modem	239137-001
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7760 Network Controller.	
Management Options	Remote Insight Lights-Out Edition II	227251-001
Security	HP/Atalla AXL600L SSL Accelerator Card for ProLiant Servers	524545-B21
Monitors	*Essential Series*	
	Compaq S9500 CRT Monitor (19-inch, Carbon/Silver)	261615-003
	Compaq S7500 CRT Monitor (17-inch, Carbon/Silver)	261606-001
	Compaq S5500 CRT Monitor (15-inch Carbon/Silver)	261602-001
	Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver)	301042-003
	Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver)	292847-003
	Advantage Series	
	Compaq V7550 CRT Color Monitor (17-inch, Carbon/Silver)	261611-003
	Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver)	295926-003
	Compaq FT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone)	301958-003
	Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver)	295925-003
	Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone)	301957-003
	Performance Series	
	HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver)	302268-003
	HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver)	302270-003
	HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver)	303486-003
	HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver)	303102-003
	Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver)	296751-003
	Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver)	285550-003
	Rackmount Flat Panel Monitors	
	TFT5110R Flat Panel Monitor (Carbon)	281683-B21
	NOTE: Monitors larger than 17" may be too heavy for use in rack systems.	

8274
A.

Options

Tape Drives

NOTE: In order to install certain tape drives internally, you may need to remove the rails that come standard on the drives and then re-insert the screws in the mounting holes. To ensure proper fit, install the mounting screws as described in the tape option kit.

Internal and External DAT Tape Drives

Internal 12/24-GB DAT Drive (Opal)	295513-B22

NOTE: Please see the 12/24-GB DAT Drive QuickSpecs for additional options such as cassettes and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10239_na/10239_na.HTML

HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, Internal (Carbon)	157769-B22
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Carbon)	157770-002
HP StorageWorks Internal 20/40-GB DAT, Hot Plug (Carbon)	215488-B21

NOTE: Please see the 20/40-GB DAT Tape Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10426_na/10426_na.HTML

Internal and External DAT 72 Tape Backup Drive

HP StorageWorks DAT 72 Tape Drive Internal (Carbon)	Q1525A
HP StorageWorks DAT 72 Tape Drive, External (Carbon)	Q1527A
HP StorageWorks DAT 72h Internal Hot Plug (Carbon)	Q1529A

NOTE: Please see the DAT 72 Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11597_na/11597_na.HTML

Internal and External LTO Ultrium Tape Drives

HP StorageWorks Ultrium 215 Tope Drive for ProLiant, Internal (Carbon)	Q1543A
HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon)	Q1544A

NOTE: Please see the HP StorageWorks Ultrium 230 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://h18006.www1.hp.com/products/quickspecs/11678_na/11678_na.html

HP StorageWorks LTO Ultrium 230 Tape Drive, Internal (Carbon)	Q1515A
HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon)	Q1516A

NOTE: Please see the HP StorageWorks LTO Ultrium QuickSpecs for additional options such as data and cleaning cartridges, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11415_na/11415_na.HTML

HP StorageWorks Ultrium 460 tape drive for ProLiant, Internal (Carbon)	Q1518A
HP StorageWorks Ultrium 460 tape drive for ProLiant, External (Carbon)	Q1519A

NOTE: Please see the HP StorageWorks Ultrium 460 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11530_na/11530_na.HTML

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 206
3698
Doc.

8213 A

Internal and External AIT Tape Drives

NOTE: The Internal AIT Hot Plug Drives are supported in hot plug drive bays only. When installing a non hot plug AIT tape drive into an ML350 ProLiant server use the special screw included with the drive kit proper fit in the removable media bay.

HP StorageWorks Internal AIT 35-GB, LVD Tape Drive (Carbon)	216884-B21
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon)	216885-001
HP StorageWorks Internal AIT 35-GB, LVD, Hot Plug (Carbon)	216886-B21

NOTE: Please see the AIT 35-GB, LVD Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10712_na/10712_na.HTML

HP StorageWorks AIT 50-GB Tape Drive, Internal (Carbon)	157766-B22
HP StorageWorks AIT 50-GB Tape Drive, External (Carbon)	157767-002
HP StorageWorks Internal AIT 50-GB, Hot Plug (carbon)	215487-B21
HP StorageWorks Rackmount AIT 50-GB, 3U (Single Drive)	274333-B21

NOTE: Please see the AIT 50-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10425_na/10425_na.HTML

HP StorageWorks Internal AIT 100-GB Tape Drive (Carbon)	249189-B21
HP StorageWorks External AIT 100-GB Tape Drive (Carbon)	249160-001
HP StorageWorks Internal AIT 100-GB, Hot-Plug (Carbon)	249161-B21

NOTE: Please see the AIT 100-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11062_na/11062_na.HTML

8272
A.

Internal and External DLT/SDLT Tape Drives	
NOTE: When installing a DLT or SDLT tape drive into a ProLiant ML350, use the special screw included with the drive kit to ensure proper fit in the removable media bay.	
HP StorageWorks 40/80-GB DLT Tape Drive, Internal (Carbon)	146196-B22
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon)	146197-B23
HP StorageWorks Rackmount DLT 40/80, 3U (Single Drive)	274332-B21
HP StorageWorks Rackmount DLT 40/80, Dual-Drive, 3U (Two Drives)	274335-B21
HP StorageWorks Rackmount DLT 40/80, Tape Array III, 5U (Four Drives)	274337-B21
NOTE: Please see the 40/80-GB DLT Drive QuickSpecs for additional options such as host bus adopters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/10658_na/10658_na.HTML	
HP StorageWorks DLT VS 40/80 Tape Drive, Internal (Carbon)	280129-B21
HP StorageWorks DLT VS 40/80 Tape Drive, External (Carbon)	280129-B22
NOTE: Please see the 40/80-GB DLT VS Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11403_na/11403_na.HTML	
HP StorageWorks SDLT 110/220, Internal (carbon)	192106-B25
HP StorageWorks SDLT 110/220, External (Carbon)	192103-002
HP StorageWorks Rackmount SDLT 110/220, 3U (Single Drive)	274331-B21
HP StorageWorks Rackmount SDLT 110/220, Dual-Drive, 3U (Two Drives)	274334-B21
HP StorageWorks Rackmount SDLT 110/220, Tape Array III, 5U (Four Drives)	274336-B21
NOTE: Please see the SDLT 110/220-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/10772_na/10772_na.HTML	
HP StorageWorks SDLT 160/320, Internal (carbon)	257319-B21
HP StorageWorks SDLT 160/320, External (carbon)	257319-001
NOTE: Please see the SDLT 160/320GB Tape Drive QuickSpecs for additional options such as adopters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11406_na/11406_na.HTML	
Internal and External DAT Autoloader	
20/40-GB DAT 8 Cassette Autoloader Internal (Opal)	166504-B21
20/40-GB DAT 8 Cassette Autoloader External (Opal)	166505-001
NOTE: Please see the 20/40-GB DAT DDS-4 8 Cassette Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/10518_na/10518_na.HTML	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 297
Page 17
Doc. 3698

Options

AIT Autoloader	
HP StorageWorks AIT 35GB Autoloader, Rackmount (carbon)	280349-001
HP StorageWorks AIT 35GB Autoloader Tabletop (carbon)	292355-001
NOTE: Please see the HP StorageWorks AIT 35GB Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11404_na/11404_na.HTML	
HP StorageWorks 1/8 Autoloader	
HP StorageWorks 1/8 Autoloader, Tabletop, Ultrium 230	C9572CB
HP StorageWorks 1/8 Autoloader, Tabletop, DLT VS80	C9264CB
HP StorageWorks 1/8 Autoloader, Rackmount kit	C9266R
NOTE: Please see the HP StorageWorks 1/8 Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11496_na/11496_na.HTML	
SSL1016 tape autoloader	
SSL1016 DLT1 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330815-B21
NOTE: Please see the SSL1016 DLT1 tape autoloader Quick Specs for additional information: http://h18000.www1.hp.com/products/quickspecs/11626_na/11626_na.HTML	
SSL1016 SDLT 160/320 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330816-B21
NOTE: Please see the SSL1016 SDLT160/320 tape autoloader Quick Specs for additional information: http://h18000.www1.hp.com/products/quickspecs/11609_na/11609_na.HTML	
Add-on drives and accessories	
SSL1016 DLT/SDLT 8-cartridge magazine	268664-B22
Rackmount Tape Drive Kits	
3U Rackmount Kit	274338-B21
NOTE: The 3U Rackmount Kit (PN 274338-B21) can support up to (2) full-height or (4) half-height tape drives and compatible with multiple Single-Ended and LVD SCSI Tape Drives including the 12/24-GB DAT, 20/40-GB DAT, DAT 72-GB, 20/40-GB DAT DDS-4 8 Cassette Autoloader, AIT 35GB LVD, AIT 50GB, AIT 100-GB, 40/80-GB DLT, DLT VS 40/80-GB, SDLT 110/220-GB, SDLT 160/320-GB, Ultrium 215, Ultrium 230 and Ultrium 460 Tape Drives.	
5U Rackmount Kit	274339-B21
NOTE: The 5U Rackmount Kit (PN 274339-B21) can support up to (4) full-height tape drives and is compatible with DLT/SDLT/LTO tape drives including the 40/80-GB DLT, SDLT 110/220, SDLT 160/320, Ultrium 230, and Ultrium 460 Tape Drives.	
NOTE: Please see the Rackmount Tape Drive Kits QuickSpecs for additional information regarding these kits, please see the following: http://www5.compaq.com/products/quickspecs/10854_na/10854_na.HTML	
Tape Storage Enclosure Cable Kits	
LVD Cable Kit, VHDCI/HD68	168048-B21
NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.	
LVD Cable Kit, HD68/HD68	242381-B21
NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.	

Options

8270
A.

Tape Automation

StorageWorks SSL2000 small system library	
SSL2020 – AIT50 based library with up to 2 drives and 20 slots	
SSL2020 AIT Mini-Library 1 drive, 20 slot Table Top	175195-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Table Top	175195-B22
SSL2020 AIT Mini-Library 1 drive, 20 slot Rackmount	175196-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Rackmount	175196-B22
SSL2020 AIT Library Pass Thru with Transport	175312-B21
Add-on drives and accessories	
SSL2020 AIT Library Pass Thru Extender	175312-B22
AIT 50GB Drive Add-On LVD Drive for SSL2020 AIT Library	175197-B21
19 Slot Magazine for SSL2020 AIT Library	175198-B21
AIT 50-GB Data Cassette (5 pack)	152841-001
AIT Cleaning Cassette	402374-B21

NOTE: Please see the SSL2020 Automated AIT Tape Library Solution QuickSpecs for additionol information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10580_na/10580_na.HTML

StorageWorks MSL6000 and MSL5000 Departmental tape libraries	
MSL6060L1 – Ultrium 460 1 based departmental library up to 4 drives and 60 slots	
MSL6060L1, 0 DRV Ultrium 460 RM Library	331196-B23
MSL6060L1, 2 DRV Ultrium 460 RM Library	331195-B21
MSL6060L1, 2 DRV Ultrium 460 TT Library	331196-B21
MSL6060L1FC, 2 DRV Ultrium 460 embedded Fibre RM Library	331196-B22

NOTE: Please see the StorageWorks MSL6060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11608_na/11608_na.HTML

StorageWorks MSL6000 and MSL5000 departmental libraries	
MSL5060L1 – LTO Ultrium 1 based departmental library up to 4 drives and 60 slots	
MSL5060L1, 0 DRV LTO1 RM Library	301899-B21
MSL5060L1, 2 DRV LTO1 RM Library	301899-B22
MSL5060L1, 2 DRV LTO1 TT Library	301900-B21
MSL5060L1FC, 2 DRV LTO1 RM-with integrated FC router	301899-B23

NOTE: Please see the StorageWorks MSL5060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11438_na/11438_no.HTML

MSL5052S2 – SDLT160 based departmental library up to 4 drives and 52 slots	
MSL5052S2, RM 0 DRV SDLT ALL	255102-B21
MSL5052S2, 2 DRV SDLT2 TT LIB	293476-B21
MSL5052S2, 2 DRV SDLT2 RM LIB	293474-B21
MSL5052S2FC 2 DRV SDLT2 RM- with integrated FC router	293474-B24

NOTE: Please see the StorageWorks MSL5052S2 Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11442_na/11442_na.HTML

RQS nº 03/2005 - CN
CPMI - - CORREIOS
298
Fls. Nº Page 19
Doc. 3698

Options

MSL6030 – LTO Ultrium 460 mid-range library up to 2 drives and 30 slots	
MSL6030 0-drive, LTO, LVDS, RM	330731-B21
MSL6030 1-drive, LTO Gen2, LVDS, RM	330731-B22
MSL6030 2-drive, LTO Gen2, LVDS, RM	330731-B23
MSL6030 1-drive, LTO Gen2, Fibre, RM	330731-B24
MSL6030 2-drive, LTO Gen2, Fibre, RM	330731-B25
MSL6030 1-drive, LTO Gen2, LVDS, TT	330788-B21
MSL6030 2-drive, LTO Gen2, LVDS, TT	330788-B22
MSL5030L1 – LTO Ultrium 1 mid-range library up to 2 drives and 30 slots	
MSL5030L1, 0 DRV LTO1 RM Library	301897-B21
MSL5030L1, 1 DRV LTO1 RM Library	301897-B22
MSL5030L1, 2 DRV LTO1 RM Library	301897-B23
MSL5030L1, 1 DRV LTO1 TT Library	301898-B21
MSL5030L1, 2 DRV LTO1 TT Library	301898-B22
MSL5030L1FC, 1 DRV LTO1 RM- with integrated FC router	301897-B24

NOTE: Please see the StorageWorks MSL5030 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11439_na/11439_na.HTML

Options

8269
A.

MSL5026S2 – SDLT160 based mid-range library up to 2 drives and 26 slots

MSL5026S2, 0 DRV SDLT2 RM Library	293472-B21
MSL5026S2, 1 DRV SDLT2 RM Library	293472-B22
MSL5026S2, 2 DRV SDLT2 RM Library	293472-B23
MSL5026S2, 1 DRV SDLT2 TT Library	293473-B21
MSL5026S2, 2 DRV SDLT2 TT Library	293473-B22
MSL5026S2FC, 1 DRV SDLT2 RM- with integrated FC router	293472-B24
MSL5026S2FC, 2 DRV SDLT2 RM- with integrated FC router	293472-B25

NOTE: Please see the StorageWorks MSL5026SL Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11453_na/11453_na.HTML

MSL5026SL Graphite – SDLT110 based mid-range library up to 2 drives and 26 slots

MSL5026SL, 1 DRV SDLT TT, graphite	302511-B21
MSL5026SL, 2 DRV SDLT TT, graphite	302511-B22
MSL5026SL, 1 DRV SDLT RM, graphite	302512-B21
MSL5026SL, 2 DRV SDLT RM, graphite	302512-B22

NOTE: Please see the StorageWorks MSL5026SL Graphite Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11440_na/11440_na.HTML

MSL5026DLX– 40/80GB DLT based mid-range library up to 2 drives and 26 slots

MSL5026DLX, 1 40/80GB DLT, LVD, TT	231821-B21
MSL5026DLX, 2 40/80GB DLT, LVD, TT	231821-B22
MSL5026DLX, 1 40/80GB DLT, LVD, RM	231891-B21
MSL5026DLX, 2 40/80GB DLT, LVD, RM	231891-B22

NOTE: Please see the StorageWorks MSL5026DLX Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10860_na/10860_na.HTML

MSL6000 and MSL5000 Add-on drives & accessories

MSL SDLT 160/320 Upgrade DRV	293475-B21
MSL Ultrium 460 upgrade drive in hot plug canister	330729-B21
MSL5000 SDLT 110/220 Upgrade DRV	231823-B22
MSL5000 40/80GB DLT Upgrade DRV	231823-B21
MSL Dual Magazine DLT (2 X 13 slot magazines)	232136-B21
MSL Universal passthrough mechanism	304825-B21
MSL 5U passthrough extender	231824-B22
MSL 10U passthrough extender	231824-B23
MSL Dual Magazine - Ultrium	301902-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
0269
Fls. Nº
3698
Doc.

Options

Smart Array Cluster Storage	Smart Array Cluster Storage	201724-B21
	Smart Array Cluster Storage Redundant Controller Option Kit	218252-B21
	128MB Cache Module for Smart Array 5302 Controller	153506-B21
	256MB Battery Backed Cache Module	254786-B21
	4-Port Shared Storage Module with Smart Array Multipath Software for Smart Array Cluster Storage	292944-B21
	NOTE: All 128MB Cache modules must be removed when 256MB cache modules are installed. NOTE: Please see the Smart Array Cluster Storage QuickSpecs for additional information including configuration steps and additional options needed for a complete solution at: http://www5.compaq.com/products/quickspecs/11050_na/11050_na.html	
External Storage – Tower and Rack	StorageWorks Enclosure Model 4314T (tower)	190210-001
	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001
	NOTE: The StorageWorks Enclosure 4300 Fomily support the Wide Ultra2/Ultra3 1" Hot Plug Hard Drives.	
	Redundant Power Supply Option	119826-B21
	Ultra3 Single Bus I/O Module Option	190212-B21
	Ultra3 Dual Bus I/O Module Option	190213-B21
	StorageWorks Enclosure Tower to Rack Conversion Kit	150213-B21
MSA1000	MSA1000	201723-B22
	MSA1000 Controller	218231-B22
	MSA Fibre Channel I/O Module	218960-B21
	MSA1000 Fabric Switch	218232-B21
	MSA1000 Fibre Channel Adapter (FCA) 2101	245299-B21
	HP StorageWorks msa hub 2/3	286763-B21
	NOTE: Please see the StorageWorks by Compaq Modulor SAN Array 1000 QuickSpecs for additional options ond configuration information at: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML	
Network Storage Router	M2402 2FCX 4SCSI LVD Network Storage Router	262653-B21
	M2402 2FCX 4SCSI HVD Network Storage Router	262654-B21
	M2402 4 channel LVD SCSI Module	262659-B21
	M2402 4 channel HVD SCSI Module	262660-B21
	M2402 2 channel FC Module	262661-B21
	MSL5000 Embedded Router Fibre Option Kit - Graphite	262672-B21
	MSL5026 Embedded Router Fibre Option Kit - Opal	286694-B21
StorageWorks Options	StorageWorks Fibre Channel SAN Switches 8-EL	176219-B21
	StorageWorks SAN Switch 2/8-EL	258707-B21
	StorageWorks SAN Switch 2/16-EL	283056-B21
	StorageWorks SAN Switch 2/8-EL Upgrade Kit	288162-B21
	StorageWorks SAN Switch 2/16-EL Upgrade Kit	288250-B21

8267
A.

Options

UPS and PDU Power Cord Matrix	**Please see the UPS and PDU cable matrix that lists cable descriptions, requirements, and specifications for UPS and PDU units:** ftp://ftp.compaq.com/pub/products/servers/ProLiantstorage/power-protection/powercordmatrix.pdf. NOTE: This Web site is available in English only.	
Uninterruptible Power Systems – Tower UPSs	HP UPS Model T700 (700VA, 500 Watt), Low Voltage	204015-001
	HP UPS T1000 XR (1000 VA, 700 Watts), Low Voltage	204155-001
	HP UPS T1500 XR (1440 VA, 1050 Watts)	204155-002
	HP UPS T2200 XR (1920 VA, 1600 Watts) Low Voltage	204451-001
	HP UPS T2200 XR (2200 VA, 1600 Watts) High Voltage	204451-002
Uninterruptible Power Systems – HP Rack UPSs	HP UPS R1500 XR (100 to 127)	204404-001
	HP UPS R3000 XR (120V)	192186-001
	HP UPS R3000 XR (208V)	192186-002
	Rack-Mountable UPS R6000 (208V) NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	347207-001
	HP UPS R12000 XR N+ x (200-240V) NOTE: The UPS R12000 XR has a hardwired input and output. NOTE: HP UPS R6000 has a hardwired input; the UPS R12000 XR has a hardwired input and output connection.	207552-B22
UPS Options	SNMP Serial Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA	192189-B21
	Six Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA.	192185-B21
	High to Low Voltage Transformer (250VA) NOTE: Supports R6000 UPS series only. 2.5A @ 125 Volts max output across two NEMA 5-15.	388643-B21
	Extended Runtime Module, T1000 XR	218967-B21
	Extended Runtime Module, T1500 XR/T2200 XR	218969-B21
	Extended Runtime Module, R1500 XR NOTE: 2U each, two ERM maximum.	218971-B21
	Extended Runtime Module, R3000 XR NOTE: 2U each, one ERM maximum.	192188-B21
	Extended Runtime Module, R6000 NOTE: 3U each, two ERM maximum.	347224-B21
	Extended Runtime Module, R12000 XR, 4U each, two ERMs maximum	217800-B21
	R12000 XR BackPlate Receptacle Kit, (2) L6-30R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-001
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-B21
	SNMP-EN Adapter NOTE: Supports R6000 UPS series only.	347225-B21
	Multi-Server UPS Card NOTE: Supports R6000 UPS series only.	123508-B21
	Scalable UPS Card NOTE: Supports R6000 UPS series only.	123509-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Options

Modular PDUs 1U/0U (Up to 32 outlets) NOTE: 1U/0U mounting brackets shipped with the unit (optimized for 10000 and 9000 series racks).	HP Modular Power Distribution Units (mPDU), Low Volt Model, 24A (100-127 VAC)	252663-D71
	NOTE: This mPDU (252663-D71) may also be used to connect the low volt model of the UPS R3000 XR.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 24A (200-240 VAC)	252663-D72
	HP Modular Power Distribution Units (mPDU), High Volt Model, 40A (200-240 VAC)	252663-B21
	NOTE: This mPDU (252663-B21), 40A model has a hardwired input.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 16A (200-240 VAC)	252663-B24
	NOTE: This PDU has a detachable input power cord and allows for adaptability to country specific power requirements. This model may also be used with the high volt UPSs R3000 XR and R6000. Order cable PN 340653-001.	
	NOTE: Please see the following Modular Power Distribution Unit (Zero-U/1U Modular PDUs) QuickSpecs for additional options including shorter jumper cables and country specific power cords: http://www5.compaq.com/products/quickspecs/11041_na/11041_na.HTML	
PDU Options	Third Party Modular PDU Modular Kit	310777-B21
	NOTE: This kit allows you to mount the Modular PDUs in (1U configuration only) in racks other than the 9000/10000 Series racks (any racks using the standard 19" rail, including the 7000 Series rocks). For more details please refer the Modular PDU QuickSpecs.	
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (1 per pock)	142257-006
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (15 per pack)	142257-007
USB Options	USB Easy Access Keyboard (carbon)	267146-008
	USB Easy Access Keyboard (carbonite)	DC168B#ABA
	USB 2-Button Scroll Mouse (carbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21
Other	Enhanced Keyboard (Carbon)	296435-005
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (HD68)	159547-B22
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (VHDCI)	333370-B21
	NOTE: The ProLiant ML330/ML350 Internal to External SCSI Cable Option Kits (PN 159547-B21 and 333370-B21) are supported by the ML330/ML350 Family.	
Rack Builder	Please see the Rack Builder for configuration assistance at http://www.compaq.com/rackbuilder/	
Rack Conversion Kit	ProLiant ML350 Generation 3 Tower to Rack Conversion Kit (CPQ branded)	290683-B21

8.266
L

Options

HP Rack 10000 Series (Graphite Metallic)	HP S10614 (14U) Rack Cabinet - Shock Pallet	292302-B22
	HP 10842 (42U) Rack Cabinet - Pallet	257415-B21
	HP 10842 (42U) Rack Cabinet - Shock Pallet	257415-B22
	HP 10647 (47U) – Pallet	245160-B21
	HP 10647 (47U) – Crated	245160-B23
	HP 10642 (42U) – Pallet	245161-B21
	HP 10642 (42U) – Shock Pallet	245161-B22
	HP 10642 (42U) – Crated	245161-B23
	HP 10636 (36U) – Pallet	245162-B21
	HP 10636 (36U) – Shock Pallet	245162-B22
	HP 10636 (36U) – Crated	245162-B23
	HP 10622 (22U) – Pallet	245163-B21
	HP 10622 (22U) – Shock Pallet	245163-B22
	HP 10622 (22U) – Crated	245163-B23
	NOTE: -B21 (pallet) used to ship empty racks shipped on a truck -B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels) -B23 (crated) used for air shipments of empty racks	
	NOTE: It is mandatory to use a shock pallet in order to ship racks with equipment installed. Not all Compaq equipment is qualified to be shipped in the Rack 10000 series.	
	NOTE: Please see the Rack 10000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color: http://www5.compaq.com/products/quickspecs/10995_na/10995_na.HTML	
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	
Compaq Rack 9000 Series (opal)	Compaq Rack 9142 (42U) – Pallet	120663-B21
	Compaq Rack 9142 (42U) – Shock Pallet	120663-B22
	Compaq Rack 9142 (42U) – Crated	120663-B23
	NOTE: –B21 (pallet) used to ship empty racks shipped on a truck –B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels) –B23 (crated) used for air shipments of empty racks	
	NOTE: Please see the Rack 9000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color: http://www5.compaq.com/products/quickspecs/10366_na/10366_na.HTML	
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html NOTE: This Web site is available in English only.	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 301
Doc.

Rack Options for HP Rack 10000 Series	Rack Blanking Panels – Graphite (Multi)	253214-B26
	NOTE: Contains one each of 1U, 2U, 4U and 8U.	
	Rack Blanking Panels – Graphite (1U)	253214-B21
	NOTE: The Rack Blanking Panels (PN 253214-B21) contains 10 each of (1U).	
	Rack Blanking Panels – Graphite (2U)	253214-B22
	NOTE: The Rack Blanking Panels (PN 253214-B22) contains 10 each of (2U).	
	Rack Blanking Panels – Graphite (3U)	253214-B23
	NOTE: The Rack Blanking Panels (PN 253214-B23) contains 10 each of (3U).	
	Rack Blanking Panels – Graphite (4U)	253214-B24
	NOTE: The Rack Blanking Panels (PN 253214-B24) contains 10 each of (4U).	
	Rack Blanking Panels – Graphite (5U)	253214-B25
	NOTE: The Rack Blanking Panels (PN 253214-B25) contains 10 each of (5U).	
	600mm Stabilizer Kit – Graphite	246107-B21
	800mm Wide Stabilizer Kit (Graphite)	255488-B21
	NOTE: Supported by the Rack 10842 cabinet only.	
	Baying Kit for Rack 10000 series (Carbon)	248929-B21
	42U Side Panel – Graphite Metallic	246099-B21
	110V Fan Kit (Graphite)	257413-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 5-15P.	
	220V Fan Kit (Graphite)	257414-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 6-15P.	
	36U Side Panel – Graphite Metallic	246102-B21
	47U Side Panel – Graphite Metallic	255486-B21
	9000/10000 Series Offset Baying Kit (42U)	248931-B21
	NOTE: This kit can be used to connect 9000 and 10000 series racks of the same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html	
	NOTE: This Web site is available in English only.	

Options

Rack Options for Compaq Rack 9000 Series	Baying/Coupling Kit	120669-B21
	42U Side Panel	120670-B21
	NOTE: The 42U Side Panel (PN 120670-B21) supports the Compaq Rock 9142 and Compaq Rack 9842.	
	36U Side Panel	120671-B21
	NOTE: The 36U Side Panel (PN 120671-B21) supports the Compaq Rock 9136.	
	600mm Stabilizer Option Kit	120673-B21
	800mm Stabilizer Option Kit (Opal)	234493-B21
	NOTE: The 800mm Stabilizer Kit (PN 234493-B21) supports the Rack 9842 only.	
	9142 Extension Kit	120679-B21
	NOTE: The 9142 Extension Kit (PN 120679-B21) supports the Campaq Rack 9142 only.	
	Stabilizer Option Kit	120673-B21
	Rack Blanking Panel Kit for Rack 9000 series (Opal) (U.S.) NOTE: The Rack Blanking Panel Kit (PN 169940-B21) contains 4 panels – one each of 1U, 2U, 4U and 8U.	169940-B21
	Rack Blanking Panels (1U) NOTE: The Rack Blanking Panels (PN 189453-B21) contains 10 each of (1U).	189453-B21
	Rack Blanking Panels (2U) NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	189453-B22
	Rack Blanking Panels (3U) NOTE: The Rack Blanking Panels (PN 189453-B23) contains 10 each of (3U).	189453-B23
	Rack Blanking Panels (4U) NOTE: The Rack Blanking Panels (PN 189453-B24) contains 10 each of (4U).	189453-B24
	Rack Blanking Panels (5U) NOTE: The Rack Blanking Panels (PN 189453-B25) contains 10 each of (5U)	189453-B25
	9136 Extension Kit	218216-B21
	9142 Short Rear Door NOTE: The 9142 Short Rear Door (PN 218217-B21) supports the Compaq Rack 9142 only.	218217-B21
	Split Rear Door (Opal) NOTE: The Split Rear Daor (PN 254045-B21) supports the 600 mm wide, 42U 9000 series rack.	254045-B21
	9136 Short Rear Door	218218-B21
	9142 Split Rear Door	254045-B21
	9000/10000 Offset Baying Kit (42U) NOTE: This kit can be used to connect 9000 and 10000 series racks of same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	248931-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

Rack Options for Compaq Rack 7000 Series	High Air Flow Rack Door Insert for the 7122 Rack	157847-B21
	High Air Flow Rack Door Insert for the 7142 Rack (single)	327281-B21
	High Air Flow Rack Door Insert for the 7142 Rack (6-pack)	327281-B22
	Compaq Networking Cable Management Kit	292407-B21
	Compaq Rack Extension Kit for 7142	154392-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 3692
Doc.

Rack Options for Rack 7000, 9000 and 10000 Series	Monitor Utility Shelf	303606-B21
	Ballast Option Kit	120672-B21
	100kg Sliding Shelf	234672-B21
	Rack Rail Adapter Kit (25-inch depth)	120675-B21
	Cable Management D-Rings Kit	168233-B21
	Console Management Controller (CMC) Option Kit	203039-B21
	Console Management Controller (CMC) Sensors Option Kit	203039-B22
	Console Management Controller (CMC) Locking Option Kit	203039-B23
	Console Management Controller (CMC) Smoke Sensors Option Kit	203039-B24
	Server Console Switch 1 x 2 port (100 to 230 VAC)	120206-001
	Server Console Switch 1 x 4 port (100 to 230 VAC)	400336-001
	Server Console Switch 1 x 8 port (100 to 230 VAC)	400337-001
	Server Console Switch 2 x 8 port (100 to 230 VAC)	400338-001
	Server Console Switch 2 x 8 port (48 VDC)	400542-B21
	IP Console Switch Box, 1x1x16	262585-B21
	IP Console Switch Box, 3x1x16	262586-B21
	IP Console Interface Adapter, 8 pack	262587-B21
	IP Console Interface Adapter, 1 pack	262588-B21
	IP Console Expansion Module	262589-B21
	KVM 9 PIN Adapter (4 Pack)	149361-B21
	CPU to Server Console Cable, 12'	110936-B21
	CPU to Server Console Cable, 20'	110936-B22
	CPU to Server Console Cable, 40'	110936-B23
	CPU to Server Console Cable, 3'	110936-B24
	CPU to Server Console Cable, 7'	110936-B25
	CPU to Server Console Cable (Plenum Rated) 20'	149363-B21
	CPU to Server Console Cable (Plenum Rated) 40'	149364-B21
	IP CAT5 Cable 3', 4 pack	263474-B21
	IP CAT5 Cable 6', 8 pack	263474-B22
	IP CAT5 Cable 12', 8 pack	263474-B23
	IP CAT5 Cable 20', 4 pack	263474-B24
	IP CAT5 Cable 40', 1 pack	263474-B25
	Switch Box Connector Kit (115 V)	144007-001
	Switch Box Connector Kit (230 V)	144007-002
	1U Rack Keyboard & Drawer (Carbon)	257054-001
	NOTE: The 1U Rack Keyboord & Drawer (PN 257054-001) is to be used with the Keyboards for Racks with Trackball (PN 158649-001).	
	TFT5600 Rack Keyboard Monitor	221546-001
	Input Device Adjustable Rails	287139-B21
	NOTE: Input Device Adjustoble Rails (287139-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Input Device Telco Roil	287138-B21
	NOTE: Input Device Telco Rails (287138-B21) are far use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Keyboard/Monitor/Mouse extension cables	169989-001
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html	
	NOTE: This Web site is available in English only.	

Options

8.262
2

HP Factory Express	*Factory Installation, Racking, and Customization Services*	
	Factory Express Server Configuration Level 1	293355-888
	NOTE: Free Installation of HP Options - Installation of HP Options memory, NICs, hard drives, controllers, processors, I/O cards, pre-install standard OEM OS image, and tape drives. Installation fees will apply to all non-HP certified hardware and asset tags. NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Server Configuration Level 2	266326-888
	NOTE: Includes Level 1 Customer Intent of a ProLiant server and options configuration, OS installation, custom image download, IP addressing, network setting, and custom packaging. Customer unique requirements (quick restore creation, cd duplication, test reports, reol-time reporting of server MAC address, password, and RILOE). Customer access, validation and control through VPN (price/server). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 3 with 1 - 3 servers or storoge enclosures	325736-888
	Factory Express Rack Integration Level 3 with 4 - 9 servers or storage enclosures	232539-888
	Factory Express Rack Integration Level 3 with 10 or more servers or storage enclosures	325735-888
	NOTE: Includes Level 1 Customer Intent for standard mounted servers and storage units plus standard cable mgmt, RAID configuration, servers & storage, power distribution, networking gear ond accessories (price/ra520ck). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 4 with 1 - 3 servers or storage enclosures	325734-888
	Factory Express Rack Integration Level 4 with 4 - 9 servers or storoge enclosures	232540-888
	Factory Express Rack Integration Level 4 with 10 or more servers or storage enclosures	325733-888
	NOTE: Includes Level 2 Customer Intent plus customer defined cable management and naming convention, customer furnished image download, IP addressing, cluster configurations (SQL, External storage RAID). Quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, RILOE). Customer access and validation through VPN (price/rock). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 5 with 1 - 3 servers or storage enclosures	325732-888
	Factory Express Rack Integration Level 5 with 4 - 9 servers or storage enclosures	232541-888
	Factory Express Rack Integration Level 5 with 10 or more servers or storage enclosures	325731-888
	NOTE: Includes Level 4 Customer Intent plus Custom SW layering and extended test, Customer access, validation and control through VPN, Clustered racks with networking gear and/or external storage array, Start-up installation services custom quote. (price/rack). NOTE: Factory Express Engineered Solution Level 6 is a custom solutions available through Factory Express. Please contact a your local reseller or Account Manager. NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
Service and Support Offerings (HP Care Pack Services)	*Hardware Services On-site Service*	
	4-Hour On-site Service, 5-Day x 13-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL3EC-36
	4-Hour On-site Service, 5-Day x 13-Hour, 3 Years (U.S. Part Number)	331045-002
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL7EC-36
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	162675-002
	6-Hour Call to Repair, On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-ELCEC-36
	6-Hour Call to Repair, On-site Service 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	331046-002

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº ~~Page 29~~ 3003
Doc. 3428

Options

Installation & Start-up Services	
Hardware Installation (Canadian Part Number)	FP-ELINS-EC
Hardware Installation (U.S. Part Number)	401791-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	240013-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-MSTEC-01
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	331051-002
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-LSTEC-01
Support Plus	
Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	239928-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-M01E1-36
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	331049-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-L01E1-36
Support Plus 24	
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number)	239930-002
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-M02E1-36
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number	331050-002
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-L02E1-36

CarePaq Priority Services for ProLiant Servers – Priority Silver	
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (2-5-2 Part Number for Canada)	FM-M04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (2-5-2 Part Number for Canada)	FM-M24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (2-5-2 Port Number for Canada)	FM-N04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (2-5-2 Part Number for Canada)	FM-N24E1-36
24 x 7 HW, 4-hr respanse, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (6-3 Part Number for U.S.)	239932-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Suppart for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	239934-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (6-3 Part Number for U.S.)	239972-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (6-3 Part Number for U.S.)	239974-002
NOTE: For more information, customer/resellers can contact http://www.hp.com/services/carepack	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 304
Doc. 3698

Memory

HP ProLiant ML350 G3 Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Array models ship standard with one 512MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

512MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models, with Advanced ECC capabilities (1x 512MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.7 GB of total memory can be implemented with the installation of three optional PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of total memory can be implemented with the removal of the standard 512-MB DIMM and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

NOTE: Charts do not represent all possible memory configurations.

		Slot 1	Slot 2	Slot 3	Slot 4
Standard	512 MB	512 MB	Empty	Empty	Empty
Optional	6656 MB	512 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB

2x1 Interleaved Memory (Recommended)		Pair 1		Pair 2	
	Total Memory	Slot 1	Slot 2	Slot 3	Slot 4
Recommended Configurations for Array Models	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

- 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB) 287494-B21
- 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB) 287495-B21
- 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB) 287496-B21

NOTE: To invoke interleaving in your array model, order this kit for a total of 1-GB of interleaved memory.

- 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB) 287497-B21
- 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB) 301044-B21

Memory

8.258

HP ProLiant ML350 G3 Non-Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

256MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities (1x 256MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.4 GB optional memory is available with the installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of memory is available with the removal of the standard 256-MB of memory and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMM installed.

NOTE: Charts do not represent all possible memory configurations

Memory					
		Slot 1	Slot 2	Slot 3	Slot 4
Standard	256 MB	256 MB	Empty	Empty	Empty
Optional	6400 MB	256 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB
Recommended Configurations for Base Models	Total Memory Desired	1	2	3	4
	512 MB	256 MB	256 MB	Empty	Empty
	1 GB	256 MB	256 MB	256 MB	256 MB
	1.5 GB	256 MB	256 MB	512 MB	512 MB
Recommended Configurations for Array models	Total Memory Desired	1	2	3	4
	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

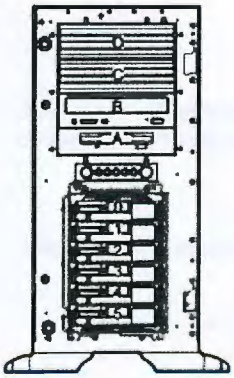
- 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB) 287494-B21
- 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB) 287495-B21

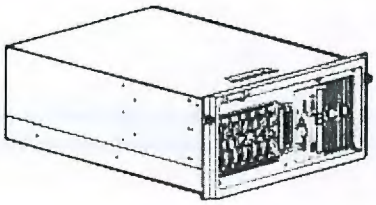
NOTE: To invoke interleaving in your base model, order this kit for a total of 512MB of interleaved memory.

- 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB) 287496-B21
- 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB) 287497-B21
- 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB) 301044-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 365
Doc. 3698

Storage





0 - 5	6 x 1 in SCSI Hard Drive Bays
A	3.5 in Diskette Drive
B	48x CD-ROM
C, D	Available half height bay

Drive Support

	Quantity Supported	Position Supported	Controller
Removable Media			
1.44-MB Diskette Drive	Up to 1	A	Integrated
IDE (ATAPI) CD-ROM Drive	Up to 2	B, C, D	Integrated IDE (ATAPI)
DVD-ROM Drive Option Kit	Up to 2	B, C, D	Integrated IDE
ML3xx Two Bay Hot Plug SCSI Drive Cage	Up to 1	C, D	Integrated SCSI

Storage

Hard Drives

Ultra320 Hot Pluggable Drives

	Quantity Supported	Position Supported	Controller
1-inch 146.8-GB 10,000 rpm 72.8-GB 10,000 rpm 36.4-GB 10,000 rpm 72.8-GB 15,000 rpm 36.4-GB 15,000 rpm 18.2-GB 15,000 rpm	Up to 6	0-5	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates.

Wide Ultra320 SCSI – Non-Hot Plug

	Quantity Supported	Position Supported	Controller
1-inch 36-GB 10,000 rpm	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

External Storage

	Quantity Supported	Position Supported	Controller
StorageWorks Enclosure 4300 [illegible] (supports [illegible]/Ultra320 1" drives)	Up to 24	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
3U Rackmount Kit 5U Rackmount Kit	Up to 3	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
MSA 1000	Please see the MSA 1000 QuickSpecs below to determine configuration requirements	External	Please see the MSA 1000 QuickSpecs (URL below) for the latest list of supported HBAs

MSA 1000: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 806
Doc. 3698

Storage

Maximum Storage Capacity – (StorageWorks Enclosure)

Internal	1.174 TB (6 x 146.8-GB 1" Ultra320 hot plug hard drives with standard internal drive cage + 2 x 72.8-GB 1²"Ultra320 Hot plug hard drive using the optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External	49.324 TB (14 x 146.8 GB) x 24
Total	50.498 TB

Tape Drives

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Drives listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10233.html

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Storage Systems listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10809.html

	Quantity Supported	Position Supported	Controller
Internal AIT 100-GB, Hot Plug Internal AIT 50-GB, Hot Plug Internal AIT 35-GB, LVD Hot Plug Internal 20/40-GB DAT Drive, Hot Plug Internal DAT 72, Hot Plug *Installation of AIT/DAT hot plug drives in D+C requires the optional Two Bay Hot Plug SCSI Drive Cage (PN 244059-B21)	Up to 3	0+ 1, 2+ 3, D+ C*	Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter *NOTE: The Smart Array 532 Controller does not support the AIT 100-GB Hot Plug Tape Drive.
20/40-GB DAT DDS-4 Tape Drive Internal 12/24-GB DAT Drive Internal DAT 72	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 35GB, Autoloader	Up to 4	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT Enhanced	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT VS	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB Internal AIT 50-GB Internal AIT 35-GB, LVD Internal	Up to 2	C, D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 230, Internal LTO Ultrium 460, Internal	Up to 1	C + D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SDLT 110/220-GB, Internal SDLT 160/320-GB, Internal	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External DAT 72	2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB External AIT 50-GB External AIT 35-GB, LVD External	2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External 40/80-GB DLT Enhanced External 40/80-GB DLT VS External 20/40-GB DLT	Up to 3	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 215, External LTO Ultrium 230, External LTO Ultrium 460, External	Up to 2	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

Storage

8-254

SDLT 110/220-GB, External SDLT 160/320-GB, External	Up to 2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
20/40-GB DAT 8 Cassette Autoloader External	Up to 1	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SSL2020 AIT Library	2 drives per SCSI channel	External	SAN Access Module for Smart Array 5302 Controller
MSL5026DLX (40/80GB DLT-based) MSL5026SL (SDLT-based) Library MSL5052SL (SDLT-based) Library MSL5030L (LTO-based) Library MSL5060S (LTO-based) Library	2 drives per SCSI channel	External	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 307
Doc. 3698

Power Specifications

Part Number	264166-001
Spare Kit	292237-001
Operational Input Voltage Range (V rms)	90 to 264
Frequency Range (Nominal) (Hz)	47 to 63 (50/60)

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Max Rated Output Wattage Rating	500	500	500	500	500	500
Nominal Input Current (A rms)	7.8	6.7	3.7	3.4	3.2	3.0
Max Rated Input Wattage Rating (Watts)	769	758	746	735	725	714
Max. Rated VA (Volt-Amp)	785	773	761	750	739	729
Efficiency (%)	65	66	67	68	68	70
Power Factor	0.98	0.98	0.98	0.98	0.98	0.98
Leakage Current (mA)	0.31	0.36	0.65	0.69	0.72	0.75
Maximum Inrush Current (A peak)	21	24	43	46	48	50
Maximum Inrush Current duration (miliseconds)	20	20	20	20	20	20

System Specifications

ML350 Generation 3 (G3) Fully Configured

Up to 2 Processors, 4 Memory Slots, 8 Hard Drives, 5 PCI Slots, and 2 Hot Plug Power Supplies

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Fully Loaded System Input Wattage (W)	557	549	541	534	526	519
Fully Loaded System Input Current (A rms)	5.7	4.9	2.7	2.5	2.3	2.2
Fully Loaded System Thermal (BTU-Hr)	1900	1872	1846	1820	1794	1770
Fully Loaded System VA (Volt-Amp)	569	560	552	545	537	530
System Leakage with all power supplies loaded (mA)	0.63	0.72	1.30	1.38	1.44	1.50
System Inrush Current with all power supplies loaded (A)	42	48	86	92	96	100
Power cord requirements	Nemo 5-15P to IEC320-C13			Option no./Spare no: See Power Cord chart		
	IEC320-C13 to IEC320-C14			Option no./Spare no: 142257-001/142258-B21		

NOTES:
ActiveAnswers Power Colculation
Power calculator is LIVE on ActiveAnswers Web site. This is an external link.
Follow this link: http://h30099.www3.hp.com/configurator/powercalcs.asp
NOTE: This Web site is available in English only.

To drill down to calculators:
- Click on: "ProLiant Servers"
- Click on the Server of interest. Example: ML350 G3
- Click on: "Power Calculatar" link. (You may need to scroll down to see it)

TechSpecs

System Unit – Tower	Dimensions (HxWxD) (with feet/bezel)	18.5 x 10.25 x 26 in (46.99 x 26.04 x 66.04 cm)	
	Dimensions (HxWxD) (without feet/bezel)	17.5 x 8.5 x 24 in (44.50 x 21.59 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 3088
Doc.

TechSpecs

System Unit – Rack	Dimensions (HxWxD)	8.61 x19 x 24 in (21.87 x48.26 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

1.44-MB Diskette Drive	LED Indicators (front panel)	Green	
	Read/Write Capacity per Diskette (high/low density)	1.44 MB/720 KB	
	Drive Supported	One	
	Drive Height	One-third	
	Drive Rotation	300 rpm	
	Transfer Rate (high/low)	500 K/250 K bits/s	
	Bytes/Sector	512	
	Sectors/Track (high/low)	18/9	
	Tracks/Side (high/low)	80/80	
	Access Times	Track-to-Track (high/low)	3/6 ms
		Average (high/low)	169/94 ms
		Settling Time	15 ms
		Latency Average	100 ms
	Cylinders (high/low)	80/80	
	Read/Write Heads	Two	

TechSpecs

8.250
L.

48X Max IDE (ATAPI) CD-ROM Drive	Disk	Applicable Disk	CD-ROM, CD-XA, CD-DA (Mode 1, Mode 2, Form 1 and 2)
			Photo CD (Single and Multi-session)
			Mixed Mode (Audio and Data combined)
			CD-R
		Capacity	540 MB (Mode 1, 12 cm)
			650 MB (Mode 2, 12 cm)
	Block Size	Mode 1	2,048 bytes
		Mode 2	2,340 bytes, 2,336 bytes
		CD-DA	2,352 bytes
		CD-XA	2,328 bytes
	Interface	IDE (ATAPI)	
	Access Times (typical)	Random	<100 ms
		Full-Stroke	<150 ms
	Data Transfer Rate	Sustained	3000 to 7200 KB/s (20X to 48X)
		Burst	150 KBps to 7,200 KBps
		Bus Rate	16.7 MBps
	Cache Buffer	128 KB	
	Start-up Time (typical)	< 7seconds	
	Stop Time	< 4seconds	
	Laser Parameters	Type	Semiconductor Laser GaA1As
		Wave Length	780 ± 25 nm
	Operating Conditions	Temperature	41° to 113° F (5° to 45° C)
		Humidity	10% to 80%
	Dimensions	(HxWxD, maximum)	1.7 x 5.85 x 8.11 in (4.29 x 14.86 x 20.60 cm)
		Weight	2.09 lb (0.95 kg)

NC7760 PCI Gigabit Server Adapter (embedded)	Network Interface	10Base-T/100Base-TX/1000Base-TX	
	Compatibility	IEEE 802.3 10Base-T	
		IEEE 802.3ab 1000Base-T	
		IEEE 80.3u 100Base-TX	
	Data Transfer Method	32-bit bus-master PCI	
	Network Transfer Rate	10Base-T(Half-Duplex)	10 Mb/s
		10Base-T(Full-Duplex)	20 Mb/s
		100Base-TX(Half-Duplex)	100 Mb/s
		100Base-TX(Full-Duplex)	200 Mb/s
		1000Base-TX	1000Mb/s
	Connector	RJ-45	
	Cable Support	10Base-T	Categories 3, 4 or 5 UTP; up to 328 ft (100 m)
		10/100/1000Base-TX	Category 5 UTP; up to 328 ft (100 m)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 309
Doc. 3698

TechSpecs

Integrated Dual Channel Wide Ultra3 SCSI Adapter	Drives Supported	Up to 28 SCSI devices (14 per channel)
	Data Transfer Method	64-bit PCI bus-master
	SCSI Channel Transfer Rate	80 MB/s per channel
	Maximum Transfer Rate per PCI Bus (peak)	133 MB/s per channel
	SCSI Protocols	Wide Ultra2 SCSI Wide-Ultra SCSI-3 Fast SCSI-2
	Electrical Protocol	Low Voltage Differential (LVD)
	SCSI Termination	Active Termination
	External SCSI Connectors	Two 80-Pin VHDCI connectors
	Internal SCSI Connectors	Two 68-Pin Wide-Ultra SCSI-3 connectors

Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with the 2.8 GHz Array Models only)	Protocol	Ultra320 SCSI
	SCSI Electrical Interface	Low Voltage Differential (LVD)
	Drives Supported	Up to 6 Ultra 320, Ultra3 and Ultra2 SCSI hard drives
	SCSI Port Connectors SA-641	one internal SCSI port
	Data Transfer Method	64-Bit PCI bus-master
	PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
	PCI	3.3 volt PCI slot compatibility only
	Simultaneous Drive Transfer Channels	Two
	Channel Transfer Rate	320-MB/s total; 320-MB/s per channel
	Software upgradeable Firmware	Yes
	Cache Memory	64-MB DRAM used for code, transfer buffers, and non-battery backed read cache
	Logical Drives Supported	32
	Maximum Capacity	880.8 GB (6 X 146.8 GB)
	Memory Addressing	64-bit, supporting servers memory greater than 4 GB
	RAID Support	RAID 5 (Distributed Data Guarding) RAID 1+ 0 (Striping & Mirroring) RAID 1 (Mirroring) RAID 0 (Striping)
	Upgradeable Firmware	2-MB Flashable ROM
	Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
	Warranty	Maximum: The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty) Minimum: One-year, on-site limited warranty Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

8.248
L.

Video Controller	Controller Chip	ATI RAGE XL
	Video DRAM	8 MB Video SDRAM
	Data Transfer Method	32-bit PCI
	Support Resolution	Supported Color Depths:
	640 x 480	16.7M, 64K, 256, 16
	800 x 600	16.7M, 64K, 256, 16
	1024 x 768	16.7M, 64K, 256, 16
	1152 x 864	16.7M, 64K, 256, 16
	1280 x 1024	16.7M, 64K, 256, 16
	1600 x 1200	64K, 256, 16
	Connector	VGA

© Copyright 2003 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation. Intel is a US registered trademark of Intel Corporation.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

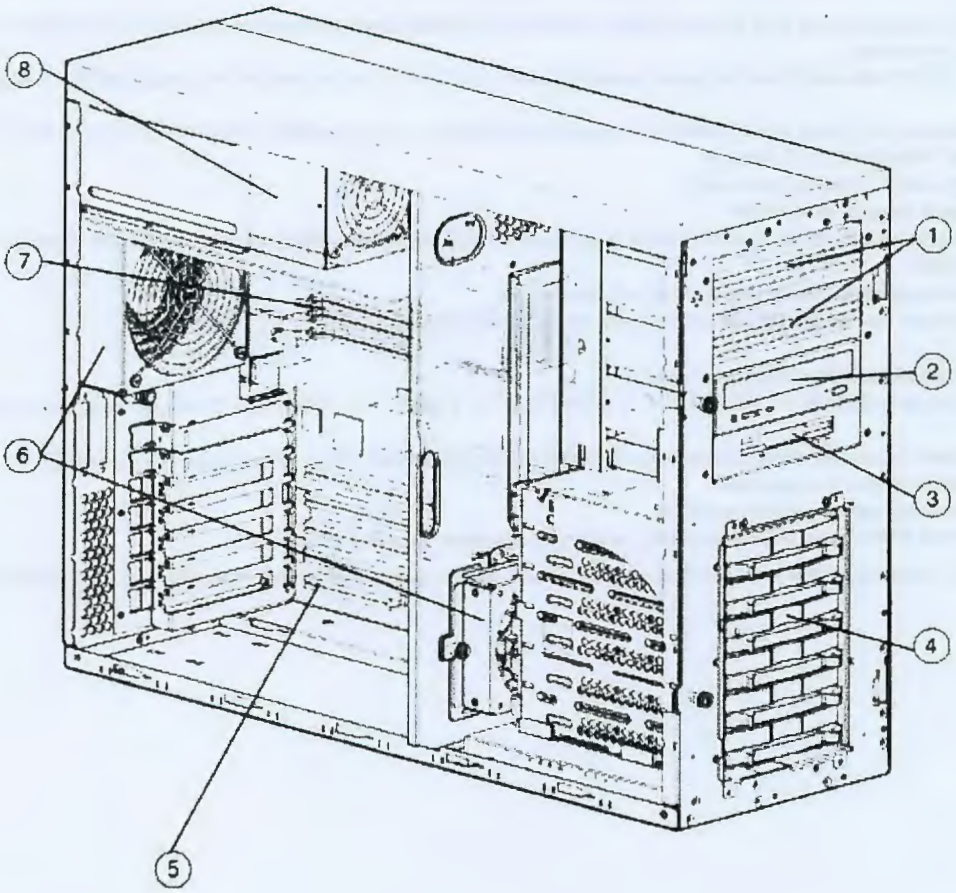
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 310
Doc. 3698

Apêndice HQ

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Overview

8.247
L.



1. Two Removable Media Bays
2. 48X Max IDE (ATAPI) CD-ROM Drive
3. 1.44 Floppy Drive
4. Six 1" Hot Plug Drive Bays
5. Five expansion slots(four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI)
6. System fan
7. DIMM sockets for up to 8GB of memory, optionally interleaved
8. Optional 2nd Power Supply for hot-pluggable 1+1 redundancy

What's New

Now available with Intel®Xeon 2.8 GHz Processors with 533MHz system bus.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº Page 1
Doc. 3698

Overview

At A Glance

- The ProLiant ML350 G3 is an expandable rack or tower platform delivering affordable 2-way performance and essential availability to corporate workgroups and growing businesses
- Intel Xeon 2.4 GHz or 2.8 GHz processors (dual processor capability) with 512-KB level 2 cache standard (full speed) and Hyper-Threading Technology
- ServerWorks Grand Champion LE Chipset with 533-MHz Front Side Bus for 2.8GHz processor models or 400-MHz FSB for models < 2.8 GHz
- Integrated Dual Channel Wide Ultra3 SCSI Adapter
- Smart Array Controller (standard in Array Models only)
- NC7760 PCI Gigabit Server Adapter (embedded)
- 512MB of 2-way interleaving capable PC2100 DDR SDRAM, with Advanced ECC capabilities (Array models only; 256MB standard on other models): Expandable to 8GB
- Flexible memory configurations allow interleaving (2x1) or non-interleaving
- Five available expansion slots: four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI
- Two USB ports
- Standard 6 x 1" Wide Ultra320 ready Hot Plug Drive Cage
- Internal storage capacity of up to 880GB (6 x 146.8 GB 1"), 1.174-TB (2 x 146.8 GB 1" + 6 x 146.8 GB 1") with optional 2-bay hot plug drive cage option
- 500W Hot-Pluggable Power Supply (standard) and an optional 500W Hot-Pluggable Redundant Power Supply (1+ 1) available
- Tool-free entry to chassis and access to components
- RBSU (ROM based setup utility) support, redundant ROM
- Insight Manager, SmartStart, ROM-based BIOS Setup Utility, and Automatic Server Recovery (ASR-2)
- Protected by HP Services, including a three-year, next business day, on-site, limited global warranty and extended Pre-Failure Warranty.

Standard Features

8.245
2.

Processor *One of the following depending on Model:*	Intel Xeon Processor 2.8 GHz/533-512KB Intel Xeon Processor 2.4 GHz/400-512KB
Cache Memory	Integrated 512-KB Level 2 cache (full speed)
Upgradability	Upgradable to dual processing
Chipset	ServerWorks Grand Champion LE Chipset with 400-MHz or 533-MHz Front Side Bus (model dependent) NOTE: For more information regarding ServerWorks, please see the following URL: http://www.serverworks.com/products/overview.html NOTE: This Web site is available in English only.
Memory (One of the following depending on model)	2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities Standard (Non-Array Models) 256MB Standard (Array Models) 512MB Maximum 8 GB
Network Controller	NC7760 Gigabit Server Adapter (embedded)
Expansion Slots	I/O (5 Total, 5 Available) 64-bit/100MHz, PCI — 4 (4 available) (Array model has 3 available) — PCI Voltage: 3.3 Volt or universal cards 32-bit/33MHz, PCI — 1 (1 available) — 5 Volt or universal cards
Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 641 Controller (2.8 GHz Array Models Only)
Storage	Diskette Drives: 1.44 MB CD-ROM: 48x IDE (ATAPI) CD-ROM Drive Hard Drives: None Maximum Internal Storage: 1.174 TB GB (6 x 146.8 GB 1" with standard internal hot plug drive cage + (2 x 146.8 GB 1") with optional ML3xx Two Bay Hot Plug SCSI Drive Cage) External Storage: Two external SCSI knockouts available, optional ProLiant ML350 Internal to External SCSI Cable Option Kit required • HD68 Internal to External SCSI Cable Option Kit PN 159547-B22 • VHDCI Internal to External SCSI Cable Option Kit PN 333370-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3215
Doc. 3691

Standard Features

Interfaces	Parallel	1
	Serial	1
	Pointing Device (Mouse)	1
	Graphics	1
	Keyboard	1
	Network RJ-45	1
	USB	2 NOTE: Please see the following URL for additional information regarding USB support: http://www.compaq.com/products/servers/platforms/usb-support.html. NOTE: This Web site is available in English only.
	External SCSI knockouts	2
Graphics	Integrated ATI RAGE XL Video Controller with 8-MB SDRAM Video Memory	
Form Factor	Tower or rack (5U) NOTE: Rack models (and rack conversion kit) support: • Square hole racks from 27"- 32" deep (including Compaq/HP 7000, 9000, 10000 and H9 series) • Square or round hole racks, from 24" - 35" deep (including HP Rack System /E and HP Systems, with an adjustment) • Telco racks with 3rd part option kit from Rack Solutions http://www.racksolutions.com/compaq/products.htm NOTE: This Web site is available in English only.	

Standard Features

ProLiant Essentials Foundation Pack Software	Insight Manager 7	Insight Manager 7 helps maximize system uptime and performance and reduces the cost of maintaining the IT infrastructure by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. Insight Manager 7 is easy to set up and provides rapid access to detailed fault and performance information gathered by the Management Agents. One-click-access to the Remote Insight Lights Out Edition II board allows systems administrators to take full graphical control of ProLiant servers in remote locations or lights-out data centers. Finally, Insight Manager 7 in concert with the Version Control Agents and Version Control Repository Manager enables systems administrators to version manage and update system software across groups of ProLiant servers.
	Management Agents	The Management Agents form the foundation for HP's Intelligent Manageability strategy. They provide direct, browser-based access to in-depth instrumentation built into HP servers, workstations, desktops, and portables, and send alerts to Insight Manager 7 and other enterprise management applications in case of subsystem or environmental failures. For additional information about the Management Agents and other management products from HP, please visit the management Web site at http://www.hp.com/servers/manage.
	SmartStart	SmartStart is a tool that simplifies server setup, providing a rapid way to deploy reliable and consistent server configurations. For more information, please visit the SmartStart website at http://www.hp.com/servers/manage. SmartStart version supported (minimum): SmartStart 5.50
	ActiveUpdate	ActiveUpdate is a web-based application that keeps IT managers directly connected to HP for proactive notification and delivery of the latest software updates.
	ROMPaq, support software, and configuration utilities	The latest software, drivers, and firmware fully optimized and tested for your ProLiant server and options.
	Survey Utility and diagnostics utilities	The most advanced configuration analysis, reporting and troubleshooting utilities used by HP and at your fingertips.
	Optional Proliant Essentials Value Packs	Optional software offerings that selectively extend the functionality of an Adaptive Infrastructure to address specific business problems and needs: • Rapid Deployment Pack – an automated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to changing business demands. • Workload Management Pack – provides easier management of complex environments, improving overall server utilization and enabling Windows 2000 customers for the first time to confidently deploy multiple applications on a single multiprocessor ProLiant Server. • Performance Management Pack – a performance management solution that identifies and explains hardware performance bottlenecks on ProLiant servers and attached options enabling users to better utilize their valuable resources.

NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information.
NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentiols
NOTE: These Web sites are available in English only.

Industry Standard Compliance	ACPI V1.0B Compliant PCI 2.2 Compliant PXE Support WOL Support PCI-X 1.0 Compliant Novell Certified Microsoft Logo certifications

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 341
Doc: 3698

Standard Features

Manageability	Insight Manager 7 Redundant ROM System Firmware Update ROMPaq Remote Insight Lights-Out Edition II (optional) ProLiant RBSU (ROM-Based Setup Utility) Automatic Server Recovery-2 (ASR-2) Drive Parameter Tracking (with Smart Array Controller) Dynamic Sector Repairing (with Smart Array Controller) Pre-Failure Warranty (covers processors, memory and hard drives)
Security	Power-on password Setup password Diskette boot control Parallel and serial interface control Disk configuration lock Power switch security
Server Power Cords	One Lowline NEMA power cord and one Highline IEC Power cord ship standard Tower models ship with standard country specific power cords. Rack models ship with IEC cables. Depending on the country, some also ship with country specific power cords Redundant power supply options ship with country specific power cords with the exception of the -B21 Rack SKU which ships with an IEC cable only.
Power Supply	500 Watts, Power Factor Correction (PFC), Hot Plug 100 to 240 VAC Rated Input Voltage (Auto-sensing), CE Mark Compliant Optional 2nd Power Supply for hot-pluggable 1 + 1 redundancy.
System Fans	2 fans ship standard, 2 fans total supported (does not include power supply fans)
Required Cabling	For required cabling information, refer to the HP Web site at http://www.hp.com/servers/proliantML350. NOTE: This Web site is available in English only.
OS Support	Microsoft Windows NT® Server 4.0 and Terminal Server 4.0 Microsoft BackOffice Small Business Server 2000 Microsoft Windows 2000 Server and Advanced Server Windows Server 2003 Novell NetWare 5.1, 6.0 Novell NetWare Small Business Suite 6.0 SCO OpenServer 5.0.6a SCO OpenUnix 8 SCO UnixWare 7.1.1 IBM OS/2 Warp Server for e-business LINUX (Red Hat, 2.1 Advanced Server, Red Hat 8.0 and Red Hat 7.3, SuSE, SLES7, UnitedLinux 1.0) NOTE: For a more complete and up-to-date listing of supported OSs and versions, please visit our OS Support Matrix at: ftp://ftp.compaq.com/pub/products/servers/os-support-matrix-310.pdf NOTE: Optional hardware may be required to support some operating systems. NOTE: For an up-to-date listing of the latest drivers available for the ProLiant ML350, please see: http://www.compaq.com/support/files/server/us/index.html. NOTE: These Web sites are available in English only.

Standard Features

8.241
L

Rack Airflow Requirements

- Rack 9000 and 10000 series Cabinets
  The increasing power of new high-performance processor technology requires increased cooling efficiency for rack-mounted servers. The 9000 and 10000 Series Racks provide enhanced airflow for maximum cooling, allowing these racks to be fully loaded with servers using the latest processors.

- Rack 7000 series Cabinets
  When installing a server with processors running at speeds of 550 MHz or greater in Rack 7000 series racks with glass doors (165753-001 (42U), and 163747-001 (22U)), the new processor technology requires the installation of HP's new High Airflow Rack Door Inserts (327281-B21 (42U), 327281-B22 (42U 6 pack), or 157847-B21 (22U)) to promote enhanced airflow for maximum cooling.

CAUTION: If a third-party rack is used, observe the following additionol requirements to ensure adequate airflow and to prevent damage to the equipment:

- Front and rear doors: If your 42U server rack includes closing front and rear doors, you must allow 830 square inches (5,350 sq cm) of hole evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).
- Side: The clearance between the installed rack component and the side panels of the rack must be a minimum of 2.75 inches (7 cm).

CAUTION: Always use blanking panels to fill all remaining empty front panel U-spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

NOTE: For additional information, refer to the Setup and Installation Guide or the Documentation CD provided with the server, or to the server documentation located in the Support section at the following URL:
http://www5.hp.com/servers/proliantml350
NOTE: This Web site is available in English only.

Installation of Server into Telco Racks

ML350 G3 rack model support: Support for all 2-post Telco racks requires the use of the rack kit and an additional option kit from Rack Solutions. http://www.racksolutions.com/compaq
NOTE: This Web site is available in English only.

HP Factory Express Capabilities

HP Factory Express gives you the flexibility to choose from a full menu of factory capabilities all in one manufacturing facility, in one process, with one touch giving you full control and access to HP's World class manufacturing facility anytime. This approach provides you the speed to deploy your IT needs, with total quality assurance, reliability, and predictability to lower your total cost of ownership by letting HP install, rack, and customize your software and hardware options for you.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 315
Page 7
Doc. 3698

Service and Support

HP Services provides a three-year, limited warranty, including Pre-Failure Warranty (coverage of hard drives, memory and processors) fully supported by a worldwide network of resellers and service providers and lifetime toll-free 7 x 24 hardware technical phone support. In addition, available service offerings include:
NOTE: Limited Warranty includes 3 year Parts, 3 year Labor, 3-year on-site support.

A full range of HP Care Pack packaged hardware and software services:

- Installation and start up
- Extended coverage hours and enhanced response times
- System management and performance services
- Availability and recovery services

NOTE: For more infomation, visit http://www.hp.com/services/carepack.

Please see the following URL regarding Warranty Information For Your HP Products:
http://www.compaq.com/support/warranty_upgrades/web_statements/176738.html.

For additional information regarding Worldwide Limited Warranty and Technical Support, please see the following URL:
ftp://ftp.compaq.com/pub/supportinformation/ejourney/176738.pdf.
NOTE: These Web sites are available in English only.

NOTE: Certain restrictions and exclusions apply. Consult the Customer Support Center at 1-800-345-1518 for details.

Models

8.239
2

ML350T03 X2.8-512KB/533, 256MB *311523-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standord (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.8-512KB/533, 256MB *311524-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)
ML350T03 X2.8-512KB/533, 512MB Array *311525-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML[illegible]R03 X2.8-512KB/533, 512MB Array *311526-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB of Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 316
Doc. 3698

Models

ML350T03 X2.4-512KB/400, 256MB 269786-001	Processor(s)	(1) Intel Xeon Processor 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)

ML350R03 X2.4-512KB/400, 256MB 269787-001	Processor(s)	(1) Xeon 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drives & drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Options

8237
A.

ProLiant ML350 G3 Unique Options	Hot Plug Redundant Power Supply Option Kit	283655-001
	Hot Plug Redundant Power Supply Option Kit (cable) NOTE: PN 283655-B21 SKU contains the 2nd power supply with an IEC power cable. Only purchase if connecting to PDU/UPS that supports IEC cables. All other SKUs contain country specific power cables.	283655-B21
	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as those with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 257913-B21) supports the ProLiant ML350 G3 servers.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This pracessor option kit (PN 283702-B21) supports the ProLiant ML350 G3 servers.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283701-B21) supports the ProLiant ML350 G3 servers.	283701-B21
	ProLiant ML350 G3 Tower to Rack Conversion Kit (CPQ brand)	290683-B21
ProLiant Essentials Value Pack Software	Rapid Deployment Pack, 1 User, V1.x NOTE: This license allows 1 server to be managed and deployed via the Deployment Server.	267196-B21
	Rapid Deployment Pack, 10 Users, V1.x NOTE: This license allows 10 servers ta be managed and deployed via the Deployment Server.	269817-B21
	Flexible Quantity License Kit	302127-B21
	License-Only - for use with a Master License Agreement	302128-B21
	ProLiant Essentials Workload Management Pack 2.0 (Featuring Compaq Resource Partitioning Manager version 2.0)	303284-B21
	ProLiant Essentials Performance Management Pack Flexible License	306697-B21
	NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information. NOTE: For more information regarding ProLiont Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials. NOTE: These Web sites are available in English only.	
HP NetServer Transition Services	HP NetServer to ProLiant integration and assessment service	304164-002
	NOTE: HP identifies current levels of NetServer support, services, and management. This service helps maximize customer's ability to add ProLiant platforms into their current environment.	
	HP TopTools to Insight Manager 7 installation and startup service	304163-002
	NOTE: Provides on-site review, installation and configuration services for Insight Manager 7. HP will also re-create, as closely as possible, the views and reports from the customer's current TopTools configuration. This service assures a smooth transition to the ProLiant Essentials software.	
	HP NetServer to ProLiant Essentials Rapid Deployment Pack installation and startup service	304162-002
	NOTE: Install and configure Rapid Deployment Pack in a test environment, then deploy a server image to a maximum of 250 systems in the production environment. This service helps to assure successful system deployment.	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Options

Processors	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiont ML350 G3 systems with 533 MHz front side bus only. This kit connot be used in 400 MHz front side bus systems such os thhose with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 257913-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiont ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283702-B21) connot be used in 533 MHz front side bus systems such os the 2.8 GHz systems.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283701-B21) cannot be used in 533 MHz front side bus systems such os the 2.8 GHz systems.	283701-B21
Memory (DIMMs)	NOTE: The ML350 G3 supports both interleaved and non-interleoved memory configurations. Base models ship standard with one 256MB DIMM or one 512MB DIMM (Array models). For best performance automatically invoke interleaving by populating memory in identical pairs. If 1GB of total memory is desired add three 256MB DIMMs to the base configuration. If 1.5GB of memory is desired add one 256MB DIMM (to pair with the standard DIMM) and two 512MB DIMMs. Interleaving and installation of memory in pairs is not required. Add any combination of memory DIMMs below to operote in non-interleaved mode. NOTE: Each SDRAM Memory kit contains one (1) DIMM.	
	128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
	256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
	512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
	1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
	2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21
Internal Storage	ML3xx Two Bay Hot Plug SCSI Drive Cage NOTE: The drive cage option kit (PN 244059-B21) has one 1" drive bay ond one 1.6" drive boy. It instolls in two avoilable removable media bays.	244059-B21
Optical Drives	16X DVD-ROM Drive Option Kit (Carbon)	217053-B21
	CD-RW/DVD-ROM 48X Combo Drive Option Kit	331346-B21
Hard Drives	*Ultra320 – Universal Hot Plug*	
	146.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286716-B22
	72.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286714-B22
	36.4-GB 10,000 rpm U320 Universal Hard Drive (1")	286713-B22
	72.8-GB 15,000 rpm U320 Universal Hard Drive (1")	286778-B22
	36.4-GB 15,000 rpm U320 Universal Hard Drive (1")	286776-B22
	18.2-GB 15,000 rpm U320 Universal Hard Drive (1")	286775-B22
	NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates. NOTE: Please see the Wide Ultra320 Universal Hot Plug QuickSpecs for additional technical information on the hard drives Support details, please see the following: http://www5.compaq.com/products/quickspecs/11531_na/11531_na.HTML	

Options

8035
A.

Storage Controllers	Smart Array 6402/128 Controller	273915-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Compaq RAID LC2 Controller	188044-B21
	Smart Array 532 Controller	225338-B21
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Ultra3 Channel Expansion Module for Smart Array 5300 Controller	153507-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-B21
	RAID ADG Upgrade for Smart Array 5302	288601-B21
	256-MB Battery Backed Cache Module NOTE: This 256-MB Battery Backed Cache Module supports the Smart Array 5300 series controllers, MSA 1000 and the Smart Array Cluster Storage.	254786-B21
	256MB Cache Upgrade for SA-6402 NOTE: This 256-MB Battery-Backed Cache Module upgrade kit supports the Smart Array 6400 series controller only.	273913-B21
	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS	284688-B21
	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter	268351-B21
	NOTE: Please see the following Controller or SCSI Adapter QuickSpecs for Technical Specifications such as PCI Bus, PCI Peak Data Transfer Rate, SCSI Protocols supported, SCSI Peak Data Transfer Rate, Channels, SCSI Ports, Drives supported, Cache, RAID support, and additional information: http://www5.compaq.com/products/quickspecs/10652_na/10652_na.HTML (RAID LC2) http://www5.compaq.com/products/quickspecs/10851_na/10851_na.HTML (Smart Array 532) http://www5.compaq.com/products/quickspecs/10640_na/10640_na.HTML (Smart Array 5300 Series) http://www5.compaq.com/products/quickspecs/11328_na/11328_na.HTML (Smart Array 5312) http://www5.compaq.com/products/quickspecs/11587_na/11587_na.HTML (Smart Array 6402) http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML (Smart Array 641) http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML (Smart Array 642) http://www5.compaq.com/products/quickspecs/10429_na/10429_na.HTML (SCSI Adapter) http://www5.compaq.com/products/quickspecs/11555_nav/11555_na.HTML (U320 Adapter)	

Wireless HAP Solution	Compaq WL410 Wireless SMB Access Point	191811-001

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 318
Page 13
3698
Doc.

Options

Communications	NC3123 Fast Ethernet NIC PCI 10/100 WOL and PXE	174830-B21
	NC3134 Fast Ethernet NIC 64 PCI Dual Port 10/100	138603-B21
	NC3135 Fast Ethernet Module Dual 10/100 Upgrade Module for NC3134	138604-B21
	NC6132 1000 SX Upgrade Module for NC3134	338456-B23
	NC6136 Gigabit Server Adapter, 64-bit/66MHz, PCI, 1000 SX	203539-B21
	NC6170 Dual Port PCI-X 1000SX Gigabit Server Adapter	313879-B21
	NC6770 PCI-X Gigabit Server Adapter, 1000-SX	244949-B21
	NC7170 Dual Port PCI-X 1000T Gigabit Server Adapter	313881-B21
	NC7132 Gigabit Upgrade Module 10/100/1000-T	153543-B21
	NC7770 PCI-X Gigabit server adapter	244948-B21
	56K v.90 PCI Modem	239137-001
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7760 Network Controller.	
Management Options	Remote Insight Lights-Out Edition II	227251-001
Security	HP/Atalla AXL600L SSL Accelerator Card for ProLiant Servers	524545-B21
Monitors	*Essential Series*	
	Compaq S9500 CRT Monitor (19-inch, Carbon/Silver)	261615-003
	Compaq S7500 CRT Monitor (17-inch, Carbon/Silver)	261606-001
	Compaq S5500 CRT Monitor (15-inch Carbon/Silver)	261602-001
	Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver)	301042-003
	Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver)	292847-003
	Advantage Series	
	Compaq V7550 CRT Color Monitor (17-inch, Carbon/Silver)	261611-003
	Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver)	295926-003
	Compaq FT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone)	301958-003
	Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver)	295925-003
	Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone)	301957-003
	Performance Series	
	HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver)	302268-003
	HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver)	302270-003
	HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver)	303486-003
	HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver)	303102-003
	Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver)	296751-003
	Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver)	285550-003
	Rackmount Flat Panel Monitors	
	TFT5110R Flat Panel Monitor (Carbon)	281683-B21
	NOTE: Monitors larger than 17" may be too heavy for use in rack systems.	

Options

8233
A.

Tape Drives

NOTE: In order to install certain tape drives internally, you may need to remove the rails that come standard on the drives and then re-insert the screws in the mounting holes. To ensure proper fit, install the mounting screws as described in the tape option kit.

Internal and External DAT Tape Drives

Internal 12/24-GB DAT Drive (Opal)	295513-B22

NOTE: Please see the 12/24-GB DAT Drive QuickSpecs for additional options such as cassettes and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10239_na/10239_na.HTML

HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, Internal (Carbon)	157769-B22
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Carbon)	157770-002
HP StorageWorks Internal 20/40-GB DAT, Hot Plug (Carbon)	215488-B21

NOTE: Please see the 20/40-GB DAT Tape Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10426_na/10426_na.HTML

Internal and External DAT 72 Tape Backup Drive

HP StorageWorks DAT 72 Tape Drive Internal (Carbon)	Q1525A
HP StorageWorks DAT 72 Tape Drive, External (Carbon)	Q1527A
HP StorageWorks DAT 72h Internal Hot Plug (Carbon)	Q1529A

NOTE: Please see the DAT 72 Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11597_na/11597_na.HTML

Internal and External LTO Ultrium Tape Drives

HP StorageWorks Ultrium 215 Tape Drive for ProLiant, Internal (Carbon)	Q1543A
HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon)	Q1544A

NOTE: Please see the HP StorageWorks Ultrium 230 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://h18006.www1.hp.com/products/quickspecs/11678_na/11678_na.html

HP StorageWorks LTO Ultrium 230 Tape Drive, Internal (Carbon)	Q1515A
HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon)	Q1516A

NOTE: Please see the HP StorageWorks LTO Ultrium QuickSpecs for additional options such as data and cleaning cartridges, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11415_na/11415_na.HTML

HP StorageWorks Ultrium 460 tape drive for ProLiant, Internal (Carbon)	Q1518A
HP StorageWorks Ultrium 460 tape drive for ProLiant, External (Carbon)	Q1519A

NOTE: Please see the HP StorageWorks Ultrium 460 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11530_na/11530_na.HTML

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 319
Doc. 3698

Internal and External AIT Tape Drives

NOTE: The Internal AIT Hot Plug Drives are supported in hot plug drive bays only. When installing a non hot plug AIT tape drive into an ML350 ProLiant server use the special screw included with the drive kit proper fit in the removable media bay.

HP StorageWorks Internal AIT 35-GB, LVD Tape Drive (Carbon)	216884-B21
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon)	216885-001
HP StorageWorks Internal AIT 35-GB, LVD, Hot Plug (Carbon)	216886-B21

NOTE: Please see the AIT 35-GB, LVD Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10712_na/10712_na.HTML

HP StorageWorks AIT 50-GB Tape Drive, Internal (Carbon)	157766-B22
HP StorageWorks AIT 50-GB Tape Drive, External (Carbon)	157767-002
HP StorageWorks Internal AIT 50-GB, Hot Plug (carbon)	215487-B21
HP StorageWorks Rackmount AIT 50-GB, 3U (Single Drive)	274333-B21

NOTE: Please see the AIT 50-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10425_na/10425_na.HTML

HP StorageWorks Internal AIT 100-GB Tape Drive (Carbon)	249189-B21
HP StorageWorks External AIT 100-GB Tape Drive (Carbon)	249160-001
HP StorageWorks Internal AIT 100-GB, Hot-Plug (Carbon)	249161-B21

NOTE: Please see the AIT 100-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11062_na/11062_na.HTML

8231
A-

Internal and External DLT/SDLT Tape Drives

NOTE: When installing a DLT or SDLT tape drive into a ProLiant ML350, use the special screw included with the drive kit to ensure proper fit in the removable media bay.

HP StorageWorks 40/80-GB DLT Tape Drive, Internal (Carbon)	146196-B22
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon)	146197-B23
HP StorageWorks Rackmount DLT 40/80, 3U (Single Drive)	274332-B21
HP StorageWorks Rackmount DLT 40/80, Dual-Drive, 3U (Two Drives)	274335-B21
HP StorageWorks Rackmount DLT 40/80, Tape Array III, 5U (Four Drives)	274337-B21

NOTE: Please see the 40/80-GB DLT Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10658_na/10658_na.HTML

HP StorageWorks DLT VS 40/80 Tape Drive, Internal (Carbon)	280129-B21
HP StorageWorks DLT VS 40/80 Tape Drive, External (Carbon)	280129-B22

NOTE: Please see the 40/80-GB DLT VS Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11403_na/11403_na.HTML

HP StorageWorks SDLT 110/220, Internal (carbon)	192106-B25
HP StorageWorks SDLT 110/220, External (Carbon)	192103-002
HP StorageWorks Rackmount SDLT 110/220, 3U (Single Drive)	274331-B21
HP StorageWorks Rackmount SDLT 110/220, Dual-Drive, 3U (Two Drives)	274334-B21
HP StorageWorks Rackmount SDLT 110/220, Tape Array III, 5U (Four Drives)	274336-B21

NOTE: Please see the SDLT 110/220-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10772_na/10772_na.HTML

HP StorageWorks SDLT 160/320, Internal (carbon)	257319-B21
HP StorageWorks SDLT 160/320, External (carbon)	257319-001

NOTE: Please see the SDLT 160/320GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11406_na/11406_na.HTML

Internal and External DAT Autoloader

20/40-GB DAT 8 Cassette Autoloader Internal (Opal)	166504-B21
20/40-GB DAT 8 Cassette Autoloader External (Opal)	166505-001

NOTE: Please see the 20/40-GB DAT DDS-4 8 Cassette Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10518_na/10518_na.HTML

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3210
Doc. 3698

AIT Autoloader	
HP StorageWorks AIT 35GB Autoloader, Rackmount (carbon)	280349-001
HP StorageWorks AIT 35GB Autoloader Tabletop (carbon)	292355-001
NOTE: Please see the HP StorageWorks AIT 35GB Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11404_na/11404_na.HTML	
HP StorageWorks 1/8 Autoloader	
HP StorageWorks 1/8 Autoloader, Tabletop, Ultrium 230	C9572CB
HP StorageWorks 1/8 Autoloader, Tabletop, DLT VS80	C9264CB
HP StorageWorks 1/8 Autoloader, Rackmount kit	C9266R
NOTE: Please see the HP StorageWorks 1/8 Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11496_na/11496_na.HTML	
SSL1016 tape autoloader	
SSL1016 DLT1 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330815-B21
NOTE: Please see the SSL1016 DLT1 tape autoloader Quick Specs for additional information: http://h18000.www1.hp.com/products/quickspecs/11626_na/11626_na.HTML	
SSL1016 SDLT 160/320 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330816-B21
NOTE: Please see the SSL1016 SDLT160/320 tape autoloader Quick Specs for additional information: http://h18000.www1.hp.com/products/quickspecs/11609_na/11609_na.HTML	
Add-on drives and accessories	
SSL1016 DLT/SDLT 8-cartridge magazine	268664-B22
Rackmount Tape Drive Kits	
3U Rackmount Kit	274338-B21
NOTE: The 3U Rackmount Kit (PN 274338-B21) can support up to (2) full-height or (4) half-height tape drives and compatible with multiple Single-Ended and LVD SCSI Tape Drives including the 12/24-GB DAT, 20/40-GB DAT, DAT 72-GB, 20/40-GB DAT DDS-4 8 Cassette Autoloader, AIT 35GB LVD, AIT 50GB, AIT 100-GB, 40/80-GB DLT, DLT VS 40/80-GB, SDLT 110/220-GB, SDLT 160/320-GB, Ultrium 215, Ultrium 230 and Ultrium 460 Tape Drives.	
5U Rackmount Kit	274339-B21
NOTE: The 5U Rackmount Kit (PN 274339-B21) can support up to (4) full-height tape drives and is compatible with DLT/SDLT/LTO tape drives including the 40/80-GB DLT, SDLT 110/220, SDLT 160/320, Ultrium 230, and Ultrium 460 Tape Drives.	
NOTE: Please see the Rackmount Tape Drive Kits QuickSpecs for additional information regarding these kits, please see the following: http://www5.compaq.com/products/quickspecs/10854_na/10854_na.HTML	
Tape Storage Enclosure Cable Kits	
LVD Cable Kit, VHDCI/HD68	168048-B21
NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Arroy III only.	
LVD Cable Kit, HD68/HD68	242381-B21
NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.	

Options

8229
A.

Tape Automation

StorageWorks SSL2000 small system library

SSL2020 – AIT50 based library with up to 2 drives and 20 slots

SSL2020 AIT Mini-Library 1 drive, 20 slot Table Top	175195-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Table Top	175195-B22
SSL2020 AIT Mini-Library 1 drive, 20 slot Rackmount	175196-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Rackmount	175196-B22
SSL2020 AIT Library Pass Thru with Transport	175312-B21

Add-on drives and accessories

SSL2020 AIT Library Pass Thru Extender	175312-B22
AIT 50GB Drive Add-On LVD Drive for SSL2020 AIT Library	175197-B21
19 Slot Magazine for SSL2020 AIT Library	175198-B21
AIT 50-GB Data Cassette (5 pack)	152841-001
AIT Cleaning Cassette	402374-B21

NOTE: Please see the SSL2020 Automated AIT Tape Library Solution QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10580_na/10580_na.HTML

StorageWorks MSL6000 and MSL5000 Departmental tape libraries

MSL6060L1 – Ultrium 460 1 based departmental library up to 4 drives and 60 slots

MSL6060L1, 0 DRV Ultrium 460 RM Library	331196-B23
MSL6060L1, 2 DRV Ultrium 460 RM Library	331195-B21
MSL6060L1, 2 DRV Ultrium 460 TT Library	331196-B21
MSL6060L1FC, 2 DRV Ultrium 460 embedded Fibre RM Library	331196-B22

NOTE: Please see the StorageWorks MSL6060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11608_na/11608_na.HTML

StorageWorks MSL6000 and MSL5000 departmental libraries

MSL5060L1 – LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL5060L1, 0 DRV LTO1 RM Library	301899-B21
MSL5060L1, 2 DRV LTO1 RM Library	301899-B22
MSL5060L1, 2 DRV LTO1 TT Library	301900-B21
MSL5060L1FC, 2 DRV LTO1 RM-with integrated FC router	301899-B23

NOTE: Please see the StorageWorks MSL5060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11438_na/11438_na.HTML

MSL5052S2 – SDLT160 based departmental library up to 4 drives and 52 slots

MSL5052S2, RM 0 DRV SDLT ALL	255102-B21
MSL5052S2, 2 DRV SDLT2 TT LIB	293476-B21
MSL5052S2, 2 DRV SDLT2 RM LIB	293474-B21
MSL5052S2FC 2 DRV SDLT2 RM- with integrated FC router	293474-B24

NOTE: Please see the StorageWorks MSL5052S2 Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11442_na/11442_na.HTML

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 321
3698
Doc.

MSL6030 – LTO Ultrium 460 mid-range library up to 2 drives and 30 slots	
MSL6030 0-drive, LTO, LVDS, RM	330731-B21
MSL6030 1-drive, LTO Gen2, LVDS, RM	330731-B22
MSL6030 2-drive, LTO Gen2, LVDS, RM	330731-B23
MSL6030 1-drive, LTO Gen2, Fibre, RM	330731-B24
MSL6030 2-drive, LTO Gen2, Fibre, RM	330731-B25
MSL6030 1-drive, LTO Gen2, LVDS, TT	330788-B21
MSL6030 2-drive, LTO Gen2, LVDS, TT	330788-B22
MSL5030L1 – LTO Ultrium 1 mid-range library up to 2 drives and 30 slots	
MSL5030L1, 0 DRV LTO1 RM Library	301897-B21
MSL5030L1, 1 DRV LTO1 RM Library	301897-B22
MSL5030L1, 2 DRV LTO1 RM Library	301897-B23
MSL5030L1, 1 DRV LTO1 TT Library	301898-B21
MSL5030L1, 2 DRV LTO1 TT Library	301898-B22
MSL5030L1FC, 1 DRV LTO1 RM- with integrated FC router	301897-B24

NOTE: Please see the StorageWorks MSL5030 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11439_na/11439_na.HTML

Options

8227
A

MSL5026S2 – SDLT160 based mid-range library up to 2 drives and 26 slots

MSL5026S2, 0 DRV SDLT2 RM Library	293472-B21
MSL5026S2, 1 DRV SDLT2 RM Library	293472-B22
MSL5026S2, 2 DRV SDLT2 RM Library	293472-B23
MSL5026S2, 1 DRV SDLT2 TT Library	293473-B21
MSL5026S2, 2 DRV SDLT2 TT Library	293473-B22
MSL5026S2FC, 1 DRV SDLT2 RM- with integrated FC router	293472-B24
MSL5026S2FC, 2 DRV SDLT2 RM- with integrated FC router	293472-B25

NOTE: Please see the StorageWorks MSL5026SL Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11453_na/11453_na.HTML

MSL5026SL Graphite – SDLT110 based mid-range library up to 2 drives and 26 slots

MSL5026SL, 1 DRV SDLT TT, graphite	302511-B21
MSL5026SL, 2 DRV SDLT TT, graphite	302511-B22
MSL5026SL, 1 DRV SDLT RM, graphite	302512-B21
MSL5026SL, 2 DRV SDLT RM, graphite	302512-B22

NOTE: Please see the StorageWorks MSL5026SL Graphite Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11440_na/11440_na.HTML

MSL5026DLX– 40/80GB DLT based mid-range library up to 2 drives and 26 slots

MSL5026DLX, 1 40/80GB DLT, LVD, TT	231821-B21
MSL5026DLX, 2 40/80GB DLT, LVD, TT	231821-B22
MSL5026DLX, 1 40/80GB DLT, LVD, RM	231891-B21
MSL5026DLX, 2 40/80GB DLT, LVD, RM	231891-B22

NOTE: Please see the StorageWorks MSL5026DLX Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10860_na/10860_na.HTML

MSL6000 and MSL5000 Add-on drives & accessories

MSL SDLT 160/320 Upgrade DRV	293475-B21
MSL Ultrium 460 upgrade drive in hot plug canister	330729-B21
MSL5000 SDLT 110/220 Upgrade DRV	231823-B22
MSL5000 40/80GB DLT Upgrade DRV	231823-B21
MSL Dual Magazine DLT (2 X 13 slot magazines)	232136-B21
MSL Universal passthrough mechanism	304825-B21
MSL 5U passthrough extender	231824-B22
MSL 10U passthrough extender	231824-B23
MSL Dual Magazine - Ultrium	301902-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 322
Doc. 3698

Options

Smart Array Cluster Storage	Smart Array Cluster Storage	201724-B21
	Smart Array Cluster Storage Redundant Controller Option Kit	218252-B21
	128MB Cache Module for Smart Array 5302 Controller	153506-B21
	256MB Battery Backed Cache Module	254786-B21
	4-Port Shared Storage Module with Smart Array Multipath Software for Smart Array Cluster Storage	292944-B21
	NOTE: All 128MB Cache modules must be removed when 256MB cache modules are installed. NOTE: Please see the Smart Array Cluster Storage QuickSpecs for additional information including configuration steps and additional options needed for a complete solution at: http://www5.compaq.com/products/quickspecs/11050_na/11050_na.html	
External Storage – Tower and Rack	StorageWorks Enclosure Model 4314T (tower)	190210-001
	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001
	NOTE: The StorageWorks Enclosure 4300 Family support the Wide Ultra2/Ultra3 1" Hot Plug Hard Drives.	
	Redundant Power Supply Option	119826-B21
	Ultra3 Single Bus I/O Module Option	190212-B21
	Ultra3 Dual Bus I/O Module Option	190213-B21
	StorageWorks Enclosure Tower to Rack Conversion Kit	150213-B21
MSA1000	MSA1000	201723-B22
	MSA1000 Controller	218231-B22
	MSA Fibre Channel I/O Module	218960-B21
	MSA1000 Fabric Switch	218232-B21
	MSA1000 Fibre Channel Adapter (FCA) 2101	245299-B21
	HP StorageWorks msa hub 2/3	286763-B21
	NOTE: Please see the StorageWorks by Compaq Modular SAN Array 1000 QuickSpecs for additional options and configuration information at: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML	
Network Storage Router	M2402 2FCX 4SCSI LVD Network Storage Router	262653-B21
	M2402 2FCX 4SCSI HVD Network Storage Router	262654-B21
	M2402 4 channel LVD SCSI Module	262659-B21
	M2402 4 channel HVD SCSI Module	262660-B21
	M2402 2 channel FC Module	262661-B21
	MSL5000 Embedded Router Fibre Option Kit - Graphite	262672-B21
	MSL5026 Embedded Router Fibre Option Kit - Opal	286694-B21
StorageWorks Options	StorageWorks Fibre Channel SAN Switches 8-EL	176219-B21
	StorageWorks SAN Switch 2/8-EL	258707-B21
	StorageWorks SAN Switch 2/16-EL	283056-B21
	StorageWorks SAN Switch 2/8-EL Upgrade Kit	288162-B21
	StorageWorks SAN Switch 2/16-EL Upgrade Kit	288250-B21

Options

8225 A

UPS and PDU Power Cord Matrix	**Please see the UPS and PDU cable matrix that lists cable descriptions, requirements, and specifications for UPS and PDU units:** ftp://ftp.compaq.com/pub/products/servers/ProLiantstorage/power-protection/powercordmatrix.pdf. NOTE: This Web site is available in English only.	
Uninterruptible Power Systems – Tower UPSs	HP UPS Model T700 (700VA, 500 Watt), Low Voltage	204015-001
	HP UPS T1000 XR (1000 VA, 700 Watts), Low Voltage	204155-001
	HP UPS T1500 XR (1440 VA, 1050 Watts)	204155-002
	HP UPS T2200 XR (1920 VA, 1600 Watts) Low Voltage	204451-001
	HP UPS T2200 XR (2200 VA, 1600 Watts) High Voltage	204451-002
Uninterruptible Power Systems – HP Rack UPSs	HP UPS R1500 XR (100 to 127)	204404-001
	HP UPS R3000 XR (120V)	192186-001
	HP UPS R3000 XR (208V)	192186-002
	Rack-Mountable UPS R6000 (208V) NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	347207-001
	HP UPS R12000 XR N+ x (200-240V) NOTE: The UPS R12000 XR has a hardwired input and output. NOTE: HP UPS R6000 has a hardwired input; the UPS R12000 XR has a hardwired input and output connection.	207552-B22
UPS Options	SNMP Serial Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA	192189-B21
	Six Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA.	192185-B21
	High to Low Voltage Transformer (250VA) NOTE: Supports R6000 UPS series only. 2.5A @ 125 Volts max output across two NEMA 5-15.	388643-B21
	Extended Runtime Module, T1000 XR	218967-B21
	Extended Runtime Module, T1500 XR/T2200 XR	218969-B21
	Extended Runtime Module, R1500 XR NOTE: 2U each, two ERM maximum.	218971-B21
	Extended Runtime Module, R3000 XR NOTE: 2U each, one ERM maximum.	192188-B21
	Extended Runtime Module, R6000 NOTE: 3U each, two ERM maximum.	347224-B21
	Extended Runtime Module, R12000 XR, 4U each, two ERMs maximum	217800-B21
	R12000 XR BackPlate Receptacle Kit, (2) L6-30R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-001
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-B21
	SNMP-EN Adapter NOTE: Supports R6000 UPS series only.	347225-B21
	Multi-Server UPS Cord NOTE: Supports R6000 UPS series only.	123508-B21
	Scaloble UPS Cord NOTE: Supports R6000 UPS series only.	123509-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 323
Doc.

Options

Modular PDUs 1U/0U (Up to 32 outlets) NOTE: 1U/0U mounting brackets shipped with the unit (optimized for 10000 and 9000 series racks).	HP Modular Power Distribution Units (mPDU), Low Volt Model, 24A (100-127 VAC) .	252663-D71
	NOTE: This mPDU (252663-D71) may also be used to connect the low volt model of the UPS R3000 XR.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 24A (200-240 VAC)	252663-D72
	HP Modular Power Distribution Units (mPDU), High Volt Model, 40A (200-240 VAC)	252663-B21
	NOTE: This mPDU (252663-B21), 40A model has a hardwired input.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 16A (200-240 VAC)	252663-B24
	NOTE: This PDU has a detachable input power cord and allows for adaptability to country specific power requirements. This model may also be used with the high volt UPSs R3000 XR and R6000. Order cable PN 340653-001.	
	NOTE: Please see the following Modular Power Distribution Unit (Zero-U/1U Modular PDUs) QuickSpecs for additional options including shorter jumper cables and country specific power cords: http://www5.compaq.com/products/quickspecs/11041_na/11041_na.HTML	
PDU Options	Third Party Modular PDU Modular Kit NOTE: This kit allows you to mount the Modular PDUs in (1U configuration only) in racks other than the 9000/10000 Series racks (any racks using the standard 19" rail, including the 7000 Series racks). For more details please refer the Modular PDU QuickSpecs.	310777-B21
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (1 per pack)	142257-006
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (15 per pack)	142257-007
USB Options	USB Easy Access Keyboard (carbon)	267146-008
	USB Easy Access Keyboard (carbonite)	DC168B#ABA
	USB 2-Button Scroll Mouse (carbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21
Other	Enhanced Keyboard (Carbon)	296435-005
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (HD68)	159547-B22
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (VHDCI) NOTE: The ProLiant ML330/ML350 Internal to External SCSI Cable Option Kits (PN 159547-B21 and 333370-B21) are supported by the ML330/ML350 Family.	333370-B21
Rack Builder	Please see the Rack Builder for configuration assistance at http://www.compaq.com/rackbuilder/	
Rack Conversion Kit	ProLiant ML350 Generation 3 Tower to Rack Conversion Kit (CPQ branded)	290683-B21

Options

8223
A.

HP Rack 10000 Series (Graphite Metallic)	HP S10614 (14U) Rack Cabinet - Shock Pallet	292302-B22
	HP 10842 (42U) Rack Cabinet - Pallet	257415-B21
	HP 10842 (42U) Rack Cabinet - Shock Pallet	257415-B22
	HP 10647 (47U) – Pallet	245160-B21
	HP 10647 (47U) – Crated	245160-B23
	HP 10642 (42U) – Pallet	245161-B21
	HP 10642 (42U) – Shock Pallet	245161-B22
	HP 10642 (42U) – Crated	245161-B23
	HP 10636 (36U) – Pallet	245162-B21
	HP 10636 (36U) – Shock Pallet	245162-B22
	HP 10636 (36U) – Crated	245162-B23
	HP 10622 (22U) – Pallet	245163-B21
	HP 10622 (22U) – Shock Pallet	245163-B22
	HP 10622 (22U) – Crated	245163-B23

NOTE: -B21 (pallet) used to ship empty racks shipped on a truck
-B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
-B23 (crated) used for air shipments of empty racks

NOTE: It is mandatory to use a shock pallet in order to ship racks with equipment installed. Not all Compaq equipment is qualified to be shipped in the Rack 10000 series.

NOTE: Please see the Rack 10000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10995_na/10995_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html
NOTE: This Web site is available in English only.

Compaq Rack 9000 Series (opal)	Compaq Rack 9142 (42U) – Pallet	120663-B21
	Compaq Rack 9142 (42U) – Shock Pallet	120663-B22
	Compaq Rack 9142 (42U) – Crated	120663-B23

NOTE: –B21 (pallet) used to ship empty racks shipped on a truck
–B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
–B23 (crated) used for air shipments of empty racks

NOTE: Please see the Rack 9000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10366_na/10366_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html
NOTE: This Web site is available in English only.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 324
Doc. 3698

Options
8222
A

Rack Options for HP Rack 10000 Series	Rack Blanking Panels – Graphite (Multi)	253214-B26
	NOTE: Contains one each of 1U, 2U, 4U and 8U.	
	Rack Blanking Panels – Graphite (1U)	253214-B21
	NOTE: The Rack Blanking Panels (PN 253214-B21) contains 10 each of (1U).	
	Rack Blanking Panels – Graphite (2U)	253214-B22
	NOTE: The Rack Blanking Panels (PN 253214-B22) contains 10 each of (2U).	
	Rack Blanking Panels – Graphite (3U)	253214-B23
	NOTE: The Rack Blanking Panels (PN 253214-B23) contains 10 each of (3U).	
	Rack Blanking Panels – Graphite (4U)	253214-B24
	NOTE: The Rack Blanking Panels (PN 253214-B24) contains 10 each of (4U).	
	Rack Blanking Panels – Graphite (5U)	253214-B25
	NOTE: The Rack Blanking Panels (PN 253214-B25) contains 10 each of (5U).	
	600mm Stabilizer Kit – Graphite	246107-B21
	800mm Wide Stabilizer Kit (Graphite)	255488-B21
	NOTE: Supported by the Rack 10842 cabinet only.	
	Baying Kit for Rack 10000 series (Carbon)	248929-B21
	42U Side Panel – Graphite Metallic	246099-B21
	110V Fan Kit (Graphite)	257413-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 5-15P.	
	220V Fan Kit (Graphite)	257414-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 6-15P.	
	36U Side Panel – Graphite Metallic	246102-B21
	47U Side Panel – Grophite Metallic	255486-B21
	9000/10000 Series Offset Baying Kit (42U)	248931-B21
	NOTE: This kit can be used to connect 9000 and 10000 series racks of the same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html	
	NOTE: This Web site is available in English only.	

Options

8221
A.

Rack Options for Compaq Rack 9000 Series	Baying/Coupling Kit	120669-B21
	42U Side Panel	120670-B21
	NOTE: The 42U Side Panel (PN 120670-B21) supports the Compoq Rack 9142 and Compaq Rack 9842.	
	36U Side Panel	120671-B21
	NOTE: The 36U Side Panel (PN 120671-B21) supports the Compaq Rack 9136.	
	600mm Stabilizer Option Kit	120673-B21
	800mm Stabilizer Option Kit (Opal)	234493-B21
	NOTE: The 800mm Stabilizer Kit (PN 234493-B21) supports the Rack 9842 only.	
	9142 Extension Kit	120679-B21
	NOTE: The 9142 Extension Kit (PN 120679-B21) supports the Compaq Rack 9142 only.	
	Stabilizer Option Kit	120673-B21
	Rack Blanking Panel Kit for Rack 9000 series (Opal) (U.S.) NOTE: The Rack Blanking Panel Kit (PN 169940-B21) contains 4 panels – one each of 1U, 2U, 4U and 8U.	169940-B21
	Rack Blanking Panels (1U) NOTE: The Rack Blanking Panels (PN 189453-B21) contains 10 each of (1U).	189453-B21
	Rack Blanking Panels (2U) NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	189453-B22
	Rack Blanking Panels (3U) NOTE: The Rack Blanking Panels (PN 189453-B23) contains 10 each of (3U).	189453-B23
	Rack Blanking Panels (4U) NOTE: The Rack Blanking Panels (PN 189453-B24) contains 10 each of (4U).	189453-B24
	Rack Blanking Panels (5U) NOTE: The Rack Blanking Panels (PN 189453-B25) contains 10 each of (5U)	189453-B25
	9136 Extension Kit	218216-B21
	9142 Short Rear Door NOTE: The 9142 Short Rear Door (PN 218217-B21) supports the Compaq Rack 9142 only.	218217-B21
	Split Rear Door (Opal) NOTE: The Split Rear Door (PN 254045-B21) supports the 600 mm wide, 42U 9000 series rack.	254045-B21
	9136 Short Rear Door	218218-B21
	9142 Split Rear Door	254045-B21
	9000/10000 Offset Baying Kit (42U) NOTE: This kit can be used to connect 9000 and 10000 series racks of same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	248931-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

Rack Options for Compaq Rack 7000 Series	High Air Flow Rack Door Insert for the 7122 Rack	157847-B21
	High Air Flow Rack Door Insert for the 7142 Rack (single)	327281-B21
	High Air Flow Rack Door Insert for the 7142 Rack (6-pack)	327281-B22
	Compaq Networking Cable Management Kit	292407-B21
	Compaq Rack Extension Kit for 7142	154392-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 325
3698
Doc.

Options

Rack Options for Rack 7000, 9000 and 10000 Series	Monitor Utility Shelf	303606-B21
	Ballast Option Kit	120672-B21
	100kg Sliding Shelf	234672-B21
	Rack Rail Adapter Kit (25-inch depth)	120675-B21
	Cable Management D-Rings Kit	168233-B21
	Console Management Controller (CMC) Option Kit	203039-B21
	Console Management Controller (CMC) Sensors Option Kit	203039-B22
	Console Management Controller (CMC) Locking Option Kit	203039-B23
	Console Management Controller (CMC) Smoke Sensors Option Kit	203039-B24
	Server Console Switch 1 x 2 port (100 to 230 VAC)	120206-001
	Server Console Switch 1 x 4 port (100 to 230 VAC)	400336-001
	Server Console Switch 1 x 8 port (100 to 230 VAC)	400337-001
	Server Console Switch 2 x 8 port (100 to 230 VAC)	400338-001
	Server Console Switch 2 x 8 port (48 VDC)	400542-B21
	IP Console Switch Box, 1x1x16	262585-B21
	IP Console Switch Box, 3x1x16	262586-B21
	IP Console Interface Adapter, 8 pack	262587-B21
	IP Console Interface Adapter, 1 pack	262588-B21
	IP Console Expansion Module	262589-B21
	KVM 9 PIN Adapter (4 Pack)	149361-B21
	CPU to Server Console Cable, 12'	110936-B21
	CPU to Server Console Cable, 20'	110936-B22
	CPU to Server Console Cable, 40'	110936-B23
	CPU to Server Console Cable, 3'	110936-B24
	CPU to Server Console Cable, 7'	110936-B25
	CPU to Server Console Cable (Plenum Rated) 20'	149363-B21
	CPU to Server Console Cable (Plenum Rated) 40'	149364-B21
	IP CAT5 Cable 3', 4 pack	263474-B21
	IP CAT5 Cable 6', 8 pack	263474-B22
	IP CAT5 Cable 12', 8 pack	263474-B23
	IP CAT5 Cable 20', 4 pack	263474-B24
	IP CAT5 Cable 40', 1 pack	263474-B25
	Switch Box Connector Kit (115 V)	144007-001
	Switch Box Connector Kit (230 V)	144007-002
	1U Rack Keyboard & Drawer (Carbon)	257054-001
	NOTE: The 1U Rack Keyboard & Drawer (PN 257054-001) is to be used with the Keyboards for Racks with Trackball (PN 158649-001).	
	TFT5600 Rack Keyboard Monitor	221546-001
	Input Device Adjustable Rails	287139-B21
	NOTE: Input Device Adjustable Rails (287139-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Input Device Telco Rail	287138-B21
	NOTE: Input Device Telco Rails (287138-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Keyboard/Monitor/Mouse extension cables	169989-001
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html	
	NOTE: This Web site is available in English only.	

Options

8219
A.

HP Factory Express	*Factory Installation, Racking, and Customization Services*	
	Factory Express Server Configuration Level 1	293355-888
	NOTE: Free Installation of HP Options - Installation of HP Options memory, NICs, hard drives, controllers, processors, I/O cords, pre-install standard OEM OS image, and tape drives. Installation fees will apply to all non-HP certified hardware and asset tags. NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Server Configuration Level 2	266326-888
	NOTE: Includes Level 1 Customer Intent of a ProLiant server and options configuration, OS installation, custom image download, IP addressing, network setting, and custom packaging. Customer unique requirements (quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, and RILOE). Customer access, validation and control through VPN (price/server). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 3 with 1 - 3 servers or storage enclosures	325736-888
	Factory Express Rack Integration Level 3 with 4 - 9 servers or storage enclosures	232539-888
	Factory Express Rack Integration Level 3 with 10 or more servers or storage enclosures	325735-888
	NOTE: Includes Level 1 Customer Intent for standard mounted servers and storage units plus standard cable mgmt, RAID configuration, servers & storage, power distribution, networking gear and accessories (price/ra520ck). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 4 with 1 - 3 servers or storage enclosures	325734-888
	Factory Express Rack Integration Level 4 with 4 - 9 servers or storage enclosures	232540-888
	Factory Express Rack Integration Level 4 with 10 or more servers or storage enclosures	325733-888
	NOTE: Includes Level 2 Customer Intent plus customer defined cable management and naming convention, customer furnished image download, IP addressing, cluster configurations (SQL, External storage RAID). Quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, RILOE). Customer access and validation through VPN (price/rack). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 5 with 1 - 3 servers or storage enclosures	325732-888
	Factory Express Rack Integration Level 5 with 4 - 9 servers or storage enclosures	232541-888
	Factory Express Rack Integration Level 5 with 10 or more servers or storage enclosures	325731-888
	NOTE: Includes Level 4 Customer Intent plus Custom SW layering and extended test, Customer access, validation and control through VPN, Clustered racks with networking gear and/or external storage orray, Stort-up installation services custom quote. (price/rack). NOTE: Factory Express Engineered Solution Level 6 is a custom solutions ovoilable through Factory Express. Please contact a your local reseller or Account Manager. NOTE: Availoble on ProLiant ML370 G3 Rack Models Only.	

Service and Support Offerings (HP Care Pack Services)	*Hardware Services On-site Service*	
	4-Hour On-site Service, 5-Day x 13-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL3EC-36
	4-Hour On-site Service, 5-Day x 13-Hour, 3 Years (U.S. Part Number)	331045-002
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL7EC-36
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	162675-002
	6-Hour Call to Repair, On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-ELCEC-36
	6-Hour Call to Repair, On-site Service 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	331046-002

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 326
Doc.

8218 A.

Installation & Start-up Services	
Hardware Installation (Canadian Part Number)	FP-ELINS-EC
Hardware Installation (U.S. Part Number)	401791-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	240013-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-MSTEC-01
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	331051-002
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-LSTEC-01
Support Plus	
Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	239928-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-M01E1-36
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	331049-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-L01E1-36
Support Plus 24	
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number)	239930-002
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-M02E1-36
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number	331050-002
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-L02E1-36

8217
A.

CarePaq Priority Services for ProLiant Servers – Priority Silver	
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (2-5-2 Part Number for Canada)	FM-M04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Suppart far Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (2-5-2 Part Number for Canada)	FM-M24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (2-5-2 Part Number for Canada)	FM-N04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (2-5-2 Part Number for Canada)	FM-N24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Monager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (6-3 Part Number for U.S.)	239932-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	239934-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (6-3 Part Number for U.S.)	239972-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (6-3 Part Number for U.S.)	239974-002
NOTE: For more information, customer/resellers can contact http://www.hp.com/services/carepack	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 327
Doc. 1698

Memory

HP ProLiant ML350 G3 Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Array models ship standard with one 512MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

512MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models, with Advanced ECC capabilities (1x 512MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect ond correct single bit memory errors while Advanced ECC extends this coverage to include protection ogoinst multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within o single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.7 GB of total memory can be implemented with the installation of three optional PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of total memory can be implemented with the removal of the standard 512-MB DIMM and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

NOTE: Charts do not represent all possible memory configurations.

		Slot 1	Slot 2	Slot 3	Slot 4
Standard	512 MB	512 MB	Empty	Empty	Empty
Optional	6656 MB	512 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB

2x1 Interleaved Memory (Recommended)		Pair 1		Pair 2	
	Total Memory	Slot 1	Slot 2	Slot 3	Slot 4
Recommended Configurations for Array Models	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following ore memory options available from HP:

- 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB) 287494-B21
- 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB) 287495-B21
- 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB) 287496-B21

NOTE: To invoke interleaving in your array model, order this kit for a total of 1-GB of interleaved memory.

- 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB) 287497-B21
- 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB) 301044-B21

Memory

8215
A.

HP ProLiant ML350 G3 Non-Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

256MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities (1x 256MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.4 GB optional memory is available with the installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of memory is available with the removal of the standard 256-MB of memory and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMM installed.

NOTE: Charts do not represent all possible memory configurations

Memory					
		Slot 1	Slot 2	Slot 3	Slot 4
Standard	256 MB	256 MB	Empty	Empty	Empty
Optional	6400 MB	256 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB

Recommended Configurations for Base Models	Total Memory Desired	1	2	3	4
	512 MB	256 MB	256 MB	Empty	Empty
	1 GB	256 MB	256 MB	256 MB	256 MB
	1.5 GB	256 MB	256 MB	512 MB	512 MB

Recommended Configurations for Array models	Total Memory Desired	1	2	3	4
	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

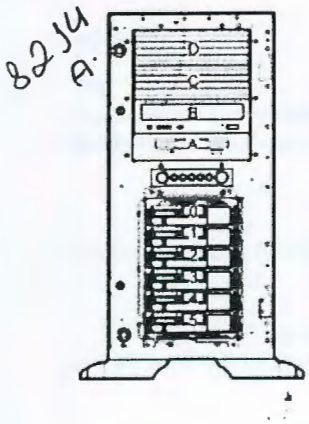
- 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB) 287494-B21
- 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB) 287495-B21

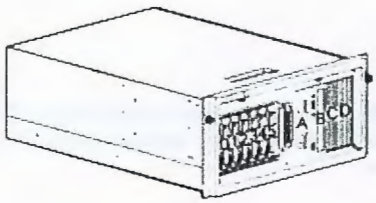
NOTE: To invoke interleaving in your base model, order this kit for a total of 512MB of interleaved memory.

- 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB) 287496-B21
- 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB) 287497-B21
- 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB) 301044-B21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Storage





0 - 5	6 x 1 in SCSI Hard Drive Bays
A	3.5 in Diskette Drive
B	48x CD-ROM
C, D	Available half height bay

Drive Support

	Quantity Supported	Position Supported	Controller
Removable Media			
1.44-MB Diskette Drive	Up to 1	A	Integrated
IDE (ATAPI) CD-ROM Drive	Up to 2	B, C, D	Integrated IDE (ATAPI)
DVD-ROM Drive Option Kit	Up to 2	B, C, D	Integrated IDE
ML3xx Two Bay Hot Plug SCSI Drive Cage	Up to 1	C, D	Integrated SCSI

Storage

Hard Drives

Ultra320 Hot Pluggable Drives

	Quantity Supported	Position Supported	Controller
1-inch 146.8-GB 10,000 rpm 72.8-GB 10,000 rpm 36.4-GB 10,000 rpm 72.8-GB 15,000 rpm 36.4-GB 15,000 rpm 18.2-GB 15,000 rpm	Up to 6	0-5	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

NOTE: All U320 Universal Hard Drives are backward compotible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates.

Wide Ultra320 SCSI – Non-Hot Plug

	Quantity Supported	Position Supported	Controller
1-inch 36-GB 10,000 rpm	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

External Storage

	Quantity Supported	Position Supported	Controller
StorageWorks Enclosure 4300 Family (supports Ultra320 1" drives)	Up to 24	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
3U Rackmount Kit 5U Rackmount Kit	Up to 3	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
MSA 1000	Please see the MSA 1000 QuickSpecs below to determine configurotion requirements	External	Please see the MSA 1000 QuickSpecs (URL below) for the latest list of supported HBAs

MSA 1000: http://www5.compaq.com/products/quickspecs/11033_na/11033_no.HTML

8013 A.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 329 3698 Doc.

Storage

Maximum Storage Capacity – (StorageWorks Enclosure)

Internal	1.174 TB (6 x 146.8-GB 1" Ultra320 hot plug hard drives with standard internal drive cage + 2 x 72.8-GB 1²"Ultra320 Hot plug hard drive using the optional ML3xx Two Bay Hat Plug SCSI Drive Cage)
External	49.324 TB (14 x 146.8 GB) x 24
Total	50.498 TB

Tape Drives

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Drives listed below, please see the following:
http://www5.compaq.com/products/quickspecs/North_America/10233.html

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Storage Systems listed below, please see the following:
http://www5.compaq.com/products/quickspecs/North_America/10809.html

	Quantity Supported	Position Supported	Controller
Internal AIT 100-GB, Hot Plug Internal AIT 50-GB, Hot Plug Internal AIT 35-GB, LVD Hot Plug Internal 20/40-GB DAT Drive, Hot Plug Internal DAT 72, Hot Plug *Installation of AIT/DAT hot plug drives in D+C requires the optional Two Bay Hot Plug SCSI Drive Cage (PN 244059-B21)	Up to 3	0+ 1, 2+ 3, D+ C*	Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter *NOTE: The Smart Array 532 Controller does not support the AIT 100-GB Hot Plug Tape Drive.
20/40-GB DAT DDS-4 Tape Drive Internal 12/24-GB DAT Drive Internal DAT 72	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 35GB, Autoloader	Up to 4	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT Enhanced	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT VS	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB Internal AIT 50-GB Internal AIT 35-GB, LVD Internal	Up to 2	C, D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 230, Internal LTO Ultrium 460, Internal	Up to 1	C + D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SDLT 110/220-GB, Internal SDLT 160/320-GB, Internal	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External DAT 72	2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB External AIT 50-GB External AIT 35-GB, LVD External	2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External 40/80-GB DLT Enhanced External 40/80-GB DLT VS External 20/40-GB DLT	Up to 3	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 215, External LTO Ultrium 230, External LTO Ultrium 460, External	Up to 2	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

8210
A.

SDLT 110/220-GB, External SDLT 160/320-GB, External	Up to 2	External	Integrated Dual Chonnel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
20/40-GB DAT 8 Cassette Autoloader External	Up to 1	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SSL2020 AIT Library	2 drives per SCSI channel	External	SAN Access Module for Smart Array 5302 Controller
MSL5026DLX (40/80GB DLT-based) MSL5026SL (SDLT-based) Library MSL5052SL (SDLT-based) Library MSL5030L (LTO-based) Library MSL5060S (LTO-based) Library	2 drives per SCSI channel	External	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 930
3698
Doc.

Power Specifications

8209 A.

Part Number	264166-001
Spare Kit	292237-001
Operational Input Voltage Range (V rms)	90 to 264
Frequency Range (Nominal) (Hz)	47 to 63 (50/60)

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Max Rated Output Wattage Rating	500	500	500	500	500	500
Nominal Input Current (A rms)	7.8	6.7	3.7	3.4	3.2	3.0
Max Rated Input Wattage Rating (Watts)	769	758	746	735	725	714
Max. Rated VA (Volt-Amp)	785	773	761	750	739	729
Efficiency (%)	65	66	67	68	68	70
Power Factor	0.98	0.98	0.98	0.98	0.98	0.98
Leakage Current (mA)	0.31	0.36	0.65	0.69	0.72	0.75
Maximum Inrush Current (A peak)	21	24	43	46	48	50
Maximum Inrush Current duration (miliseconds)	20	20	20	20	20	20

System Specifications

ML350 Generation 3 (G3) Fully Configured						
Up to 2 Processors, 4 Memory Slots, 8 Hard Drives, 5 PCI Slots, and 2 Hot Plug Power Supplies						
Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Fully Loaded System Input Wattage (W)	557	549	541	534	526	519
Fully Loaded System Input Current (A rms)	5.7	4.9	2.7	2.5	2.3	2.2
Fully Loaded System Thermal (BTU-Hr)	1900	1872	1846	1820	1794	1770
Fully Loaded System VA (Volt-Amp)	569	560	552	545	537	530
System Leakage with all power supplies loaded (mA)	0.63	0.72	1.30	1.38	1.44	1.50
System Inrush Current with all power supplies loaded (A)	42	48	86	92	96	100
Power cord requirements	Nema 5-15P to IEC320-C13			Option no./Spare no: See Power Cord chart		
	IEC320-C13 to IEC320-C14			Option no./Spare no: 142257-001/142258-B21		

NOTES:
ActiveAnswers Power Calculation
Power calculator is LIVE on ActiveAnswers Web site. This is an external link.
Follow this link: http://h30099.www3.hp.com/configurator/powercalcs.asp
NOTE: This Web site is available in English only.

To drill down to calculators:
- Click on: "ProLiant Servers"
- Click on the Server of interest. Example: ML350 G3
- Click on: "Power Calculator" link. (You may need to scroll down to see it)

TechSpecs

System Unit – Tower	Dimensions (HxWxD) (with feet/bezel)	18.5 x 10.25 x 26 in (46.99 x 26.04 x 66.04 cm)	
	Dimensions (HxWxD) (without feet/bezel)	17.5 x 8.5 x 24 in (44.50 x 21.59 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

8208
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Page 39
Fls. Nº 33
3698
Doc.

TechSpecs

System Unit – Rack	Dimensions (HxWxD)	8.61 x19 x 24 in (21.87 x48.26 x 60.96 cm)	
8707 A'	Weight(approximate)	60 lb (27.24 kg) (without hord drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors	
		(Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

1.44-MB Diskette Drive	LED Indicators (front panel)	Green	
	Read/Write Capacity per Diskette (high/low density)	1.44 MB/720 KB	
	Drive Supported	One	
	Drive Height	One-third	
	Drive Rotation	300 rpm	
	Transfer Rate (high/low)	500 K/250 K bits/s	
	Bytes/Sector	512	
	Sectors/Track (high/low)	18/9	
	Tracks/Side (high/low)	80/80	
	Access Times	Track-to-Track (high/low)	3/6 ms
		Average (high/low)	169/94 ms
		Settling Time	15 ms
		Latency Average	100 ms
	Cylinders (high/low)	80/80	
	Read/Write Heads	Two	

TechSpecs

8206
A

48X Max IDE (ATAPI) CD-ROM Drive	Disk	Applicable Disk	CD-ROM, CD-XA, CD-DA (Mode 1, Mode 2, Form 1 and 2)
			Photo CD (Single and Multi-session)
			Mixed Mode (Audio and Data combined)
			CD-R
		Capacity	540 MB (Mode 1, 12 cm)
			650 MB (Mode 2, 12 cm)
	Block Size	Mode 1	2,048 bytes
		Mode 2	2,340 bytes, 2,336 bytes
		CD-DA	2,352 bytes
		CD-XA	2,328 bytes
	Interface	IDE (ATAPI)	
	Access Times (typical)	Random	<100 ms
		Full-Stroke	<150 ms
	Data Transfer Rate	Sustained	3000 to 7200 KB/s (20X to 48X)
		Burst	150 KBps to 7,200 KBps
		Bus Rate	16.7 MBps
	Cache Buffer	128 KB	
	Start-up Time (typical)	< 7seconds	
	Stop Time	< 4seconds	
	Laser Parameters	Type	Semiconductor Laser GaA1As
		Wave Length	780 ± 25 nm
	Operating Conditions	Temperature	41° to 113° F (5° to 45° C)
		Humidity	10% to 80%
	Dimensions	(HxWxD, maximum)	1.7 x 5.85 x 8.11 in (4.29 x 14.86 x 20.60 cm)
		Weight	2.09 lb (0.95 kg)

NC7760 PCI Gigabit Server Adapter (embedded)	Network Interface	10Base-T/100Base-TX/1000Base-TX	
	Compatibility	IEEE 802.3 10Base-T	
		IEEE 802.3ab 1000Base-T	
		IEEE 80.3u 100Base-TX	
	Data Transfer Method	32-bit bus-master PCI	
	Network Transfer Rate	10Base-T(Half-Duplex)	10 Mb/s
		10Base-T(Full-Duplex)	20 Mb/s
		100Base-TX(Half-Duplex)	100 Mb/s
		100Base-TX(Full-Duplex)	200 Mb/s
		1000Base-TX	1000Mb/s
	Connector	RJ-45	
	Cable Support	10Base-T	Categories 3, 4 or 5 UTP; up to 328 ft (100 m)
		10/100/1000Base-TX	Category 5 UTP; up to 328 ft (100 m)

RQS nº 03/2005 - CN
CPMI - CORREIOS
232
Fls Nº:
Doc. 3698

Integrated Dual Channel Wide Ultra3 SCSI Adapter	Drives Supported	Up to 28 SCSI devices (14 per channel)
	Data Transfer Method	64-bit PCI bus-master
	SCSI Channel Transfer Rate	80 MB/s per channel
	Maximum Transfer Rate per PCI Bus (peak)	133 MB/s per channel
	SCSI Protocols	Wide Ultra2 SCSI Wide-Ultra SCSI-3 Fast SCSI-2
	Electrical Protocol	Low Voltage Differential (LVD)
	SCSI Termination	Active Termination
	External SCSI Connectors	Two 80-Pin VHDCI connectors
	Internal SCSI Connectors	Two 68-Pin Wide-Ultra SCSI-3 connectors

Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with the 2.8 GHz Array Models only)	Protocol	Ultra320 SCSI
	SCSI Electrical Interface	Low Voltage Differential (LVD)
	Drives Supported	Up to 6 Ultra 320, Ultra3 and Ultra2 SCSI hard drives
	SCSI Port Connectors SA-641	one internal SCSI port
	Data Transfer Method	64-Bit PCI bus-master
	PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
	PCI	3.3 volt PCI slot compatibility only
	Simultaneous Drive Transfer Channels	Two
	Channel Transfer Rate	320-MB/s total; 320-MB/s per channel
	Software upgradeable Firmware	Yes
	Cache Memory	64-MB DRAM used for code, transfer buffers, and non-battery backed read cache
	Logical Drives Supported	32
	Maximum Capacity	880.8 GB (6 X 146.8 GB)
	Memory Addressing	64-bit, supporting servers memory greater than 4 GB
	RAID Support	RAID 5 (Distributed Data Guarding) RAID 1+ 0 (Striping & Mirroring) RAID 1 (Mirroring) RAID 0 (Striping)
	Upgradeable Firmware	2-MB Flashable ROM
	Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
	Warranty	Maximum: The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty) Minimum: One-year, on-site limited warranty Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

TechSpecs

8204
A.

Video Controller	Controller Chip	ATI RAGE XL
	Video DRAM	8 MB Video SDRAM
	Data Transfer Method	32-bit PCI
	Support Resolution	Supported Color Depths:
	640 x 480	16.7M, 64K, 256, 16
	800 x 600	16.7M, 64K, 256, 16
	1024 x 768	16.7M, 64K, 256, 16
	1152 x 864	16.7M, 64K, 256, 16
	1280 x 1024	16.7M, 64K, 256, 16
	1600 x 1200	64K, 256, 16
	Connector	VGA

© Copyright 2003 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation. Intel is a US registered trademark of Intel Corporation.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº Page 43
Doc. 3698

Apêndice HR

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3341
Doc. 3698

Cisco Systems

8202
A.

Overview

CiscoWorks **VPN/Security Management** Solution Version 2.2

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE Blueprint from Cisco for network security. CiscoWorks VMS protects the productivity and reduces operating costs for enterprises, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments.

Today's business challenges and resulting security deployments require more scalability than merely supporting a large number of devices. Many customers have limited staffing, yet are asked to manage a myriad of security devices. These customers must manage the security and network infrastructure; frequently update many remote devices; implement change control and auditing when multiple organizations are involved in defining and deploying policies; enhance security without adding more headcount; or roll out remote access VPNs to all employees and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from a small to large environment, using the following multifaceted scalability features:

- Complete SAFE Blueprint Coverage

  To completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or Cisco IOS® Software, and support a range of management functions. CiscoWorks VMS is uniquely able to scale across SAFE Blueprint components, including firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS also takes advantage of Cisco Secure Access Control Server (ACS) by using a common ACS logon. CiscoWorks VMS can manage a feature set through an appliance, for example, the Cisco PIX® Firewall, or through the Cisco IOS Software. Scalable management also involves more than configuring devices. CiscoWorks VMS provides the complete range of management with features to configure, monitor, and troubleshoot the network.
- Scalable Foundation

  CiscoWorks VMS implements a foundation with a consistent user experience, which makes it easier to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI, workflow, ACS logon, roles definition, platforms, database

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 335
3698
Doc.

engine, installation, and more. An industry-leading feature of this foundation is the Auto Update feature, which allows numerous devices to be updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and "pull" the most current security configurations or Cisco PIX operating system. Auto Update is required to effectively scale remote office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a "push" model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update a more manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations. In addition to easier and faster policy updates, Auto Update also provides consistent policy deployments.

- Enterprise Operational Integration

  CiscoWorks VMS enables organizations to easily integrate management into their operations. One operational need is to replicate policies to multiple locations. The Smart Rules hierarchy addresses this need, by enabling administrators to define device groups and implement policy inheritance. For example, an administrator can define a device group for the New York sales office and deploy that same policy to all other sales offices quickly and consistently. The Command and Control Workflow feature provides change control and auditing, and is particularly important for customers who have separate groups for network and security operations. The solution includes processes for generating, approving, and deploying configurations. This can help security operations to define and approve new policies. Network operations can later deploy the new policies during their regular maintenance window. An audit of the changes can be maintained.

- Centralized Role-Based Access Control (RBAC)

  Role-based access control enables organizations to scale access privileges. CiscoWorks VMS conveniently uses a common ACS logon for users, administrators, devices, and applications. CiscoWorks VMS enables different groups to have different access rights across different devices and applications.

- Integrated Infrastructure Management

  Scalability requires that multiple components be managed, not just firewalls, but also VPNs, network- and host-based IDSs, routers, and switches. CiscoWorks VMS not only manages the security infrastructure, but also manages the network infrastructure. Customers benefit from being able to manage these components from one solution. Integrated monitoring is also required to see the larger picture. CiscoWorks VMS provides integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDSs, along with event correlation.

CiscoWorks VMS Functions

CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

- Firewall management
- Auto Update Server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

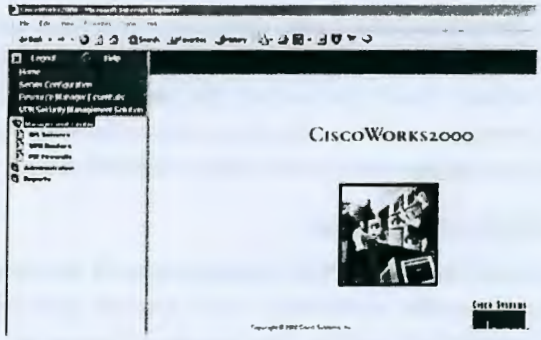
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8200
A.

These functional areas supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.

Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard.

Figure 1



Firewall Management

CiscoWorks VMS enables the large-scale deployment of Cisco PIX firewalls, by providing the following features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access with administrative privileges per device and customer groups with other CiscoWorks products and Cisco Secure ACS
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory, or Auto Update Server
- Look and feel of Cisco PIX Device Manager but with scalability to thousands of PIX firewalls
- Integration with other CiscoWorks network management software
- Complete SAFE Blueprint coverage for centralized management of Cisco PIX firewalls, including access control, VPN, IDS, and authentication, authorization, and accounting (AAA)

Smart Rules is an innovative feature that allows common information including access rules and settings to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, which results in reduced configuration time, fewer administrative errors, and higher device scalability. Using Smart Rules, a user can configure a common rule such as allowing all HTTP traffic once and can apply this rule globally to all firewalls. Smart Rules can also be defined on a device or customer group basis. For specific information on the firewall management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html

Auto Update Server for Firewall Management

CiscoWorks VMS introduces the industry's first firewall Auto Update Server that allows users to implement a "pull" model for security and Cisco PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls to both periodically and automatically contact the update server for any security configuration, Cisco PIX Operating System, and PIX Device Manager (PDM) updates. The Auto Update Server supports the following features:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 320
Doc. 3698

8399
A

- Security management of remote Cisco PIX firewalls that use Dynamic Host Control Protocol (DHCP)
- Automated Cisco PIX OS distribution to groups of Cisco PIX firewalls
- Automated Cisco PDM updates to remote firewalls
- Configuration verification at periodic intervals
- Automated replacement of inaccurate or tampered configurations
- New firewalls configured at "boot time"

The Auto Update Server is an indispensable component of any large-scale remote Cisco PIX firewall deployment. Auto Update Server is an easy-to-use solution to automatically update all remote or local firewalls with new operating system releases. Cisco is the industry's first vendor to provide this pull model of security policy and operating system management. For specific information on the Auto Update Server component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3993/index.html

Network-Based IDS Management

Administrators can use CiscoWorks VMS to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles. Additionally, a more powerful signature management feature is included to increase the accuracy and specificity of detection. Some prominent features are:

- Easy-to-use Web-based interface
- Wizards that lead users through common management tasks
- Access to the Network Security Database (NSDB), which provides meaningful information about alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups, and the ability to configure multiple sensors concurrently using group profiles
- Support for several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

For specific information on the network-based IDS management functionality of VMS, refer to:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

Host-Based IDS Management

CiscoWorks VMS provides threat protection for server and desktop computing systems, also known as "endpoints." VMS goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because CiscoWorks VMS analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Features of host-based IDS management include:

- Aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent.
- Provides preventive protection against entire classes of attacks including port scans, buffer overflows, Trojan horses, malformed packets, and e-mail worms.
- Offers "zero update" prevention for known and unknown attacks

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Provides industry-leading protection for UNIX and Windows servers and Windows desktops allowing customers to patch systems on their own schedules.
- Open and extensible architecture offers the capability to define and enforce security according to corporate policy.
- Scalable to thousands of agents per manager to support large enterprise deployments.

For specific information on the host-based IDS management functionality of VMS, refer to: the Management Center for Cisco Security Agents Datasheet.

VPN Router Management

CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This application is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPsec) tunneling policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunneling policies.
- Hierarchical inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keepalive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized role-based access control model allows for centralized management of users and accounts.

For specific information on the VPN router management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/index.html

Security Monitoring

CiscoWorks VMS provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a broader view of security status.

- Integrated monitoring is used to capture, store, view, correlate, and report on events from many of the devices in the SAFE Blueprint such as Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.
- Event correlation is used to identify attacks that are not easily recognizable from a single event. A flexible notification scheme and automated responses to critical events also aid in quick action.
- The event viewer can read both real-time and historical events.
- Events are color-coded and administrators can quickly isolate problems. Administrators can also define thresholds and time periods when rules can be triggered to provide notification.
- On-demand and scheduled reports facilitate ongoing monitoring.

For specific information on the security monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3991/index.html

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 337
Doc. 3698

VPN Monitoring

CiscoWorks VMS offers a Web-based management tool that allows network administrators to collect, store, and view information on IPsec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. This dashboard provides the following capabilities:

- Provides data on system resources related to real-time memory usage, percent CPU usage per device, and active tunnel and active sessions. This data simplifies the identification of devices with potential performance problems and devices with the highest usage.
- Enables viewing of current and long-term packet rates and packet dropped percentage which can aid in determining where excess capacity can be tapped or quickly identify bottlenecks and device throughput problems.
- Enables identification of the devices with the most persistent problems through the event log; key device and VPN statistics are evaluated against a set of global and device-specific thresholds, and exceptions are recorded in the event log.
- Provides graphing of important common metrics. Device performance comparisons provide a global view of short-term trends in VPN performance, enabling administrators to identify problem areas before they become critical failures.

For specific information on the VPN monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2326/index.html

Operational Management

CiscoWorks VMS provides the operational management for the network, allowing network managers to perform the following:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report on hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources
- Quickly identify devices that can be used for VPNs, if upgraded with the appropriate Cisco IOS Software
- Discover which VPN devices have hardware encryption modules
- Graphically compare configurations of VPN devices
- Isolate IPsec-related problems by running customized Syslog reports

For specific information on the operational management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html

Server Specifications (Minimum requirements)

Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- Sun UltraSPARC 60 MP with 440 MHz or faster processor
- Sun UltraSPARCIII (Sun Blade 2000 Workstation or Sun Fire 280R Workgroup Server)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8196
A.

- CD-ROM drive
- 100BASE-T or faster connection
- 1 GB RAM
- 9 GB available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit color

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Sun Solaris 2.8 with patches:

109742 has been replaced by 108528-13

109322 has been replaced by 108827-15

109279 has been replaced by 108528-13

108991 has been replaced by 108827-15

Java Requirements

Sun Java plug-in 1.3.1-b24

Client Requirements

Hardware

- PC-compatible computer with 300 MHz or faster Pentium processor
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.
- Solaris 2.8

Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems
- Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

The CiscoWorks Management Center for Firewalls, and CiscoWorks Management Center for VPN Routers, are supported on Internet Explorer 6.0, but not on Netscape Navigator. In addition to supporting Internet Explorer The Management Center for IDS and the Monitoring Center for Security are also supported on Netscape Navigator.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 339
3696
Doc.

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. CiscoWorks VMS includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation.

For More Information

For more information, go to http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/ or send e-mail to ciscoworks@cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, Cisco Unity, and EtherSwitch are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203051/ETMG 04/03

Apêndice HS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 339
Doc. 3698

8194
A.

CHAPTER 12

Administrators and Administrative Policy

This chapter addresses the Cisco Secure Access Control Server (Cisco Secure ACS) Appliance version 3.2 features found in the Administration Control section of the HTML interface. It contains the following sections:

- Administrator Accounts, page 12-1
- Access Policy, page 12-11
- Session Policy, page 12-16

Administrator Accounts

This section provides details about Cisco Secure ACS administrators. It contains the following topics:

- About Administrator Accounts, page 12-2
- Administrator Privileges, page 12-2
- Adding an Administrator Account, page 12-6
- Editing an Administrator Account, page 12-8
- Unlocking a Locked Out Administrator Account, page 12-10
- Deleting an Administrator Account, page 12-11

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 310
Doc. 3698

About Administrator Accounts

Administrators are the only users of the Cisco Secure ACS HTML interface. To access the Cisco Secure ACS HTML interface from a browser, you must log in to Cisco Secure ACS using an administrator account.

Note Cisco Secure ACS administrator accounts are unique to Cisco Secure ACS. They are not related to administrator accounts for your network, operating systems, or other software.

In the HTML interface, an administrator can configure any of the features provided in Cisco Secure ACS; however, the ability to access various parts of the HTML interface can be limited by revoking privileges to those parts of the HTML interface that a given administrator is not permitted to access.

For example, you may want to limit access to the Network Configuration section of the HTML interface to the administrators whose responsibilities include network management. To do so, you would select only the Network Configuration privilege for the applicable administrator accounts. For more information about administrator privileges, see Administrator Privileges, page 12-2.

Cisco Secure ACS administrator accounts have no correlation with Cisco Secure ACS user accounts or network user authentication. Cisco Secure ACS stores accounts created for authentication of network service requests and those created for Cisco Secure ACS administrative access in separate internal databases.

Administrator Privileges

You can grant appropriate privileges to each Cisco Secure ACS administrator by assigning privileges on an administrator-by-administrator basis. You control privileges by selecting the options in the Administrator Privileges table on the Add Administrator or Edit Administrator pages. These options are listed below:

- **User and Group Setup**—Contains the following privilege options for the User Setup and Group Setup sections of the HTML interface:
  - **Add/Edit users in these groups**—Enables the administrator to add or edit users and to assign users to groups in the Editable groups list.

- **Setup of these groups**—Enables the administrator to edit the settings for the groups in the Editable groups list.
- **Available Groups**—Lists the user groups for which the administrator *does not* have edit privileges and to which the administrator *cannot* add users.
- **Editable Groups**—Lists the user groups for which the administrator *does* have edit privileges and to which the administrator account *can* add users.

- **Shared Profile Components**—Contains the following privilege options for the Shared Profile Components section of the HTML interface:
  - **Network Access Restriction Sets**—Allows the administrator full access to the Network Access Restriction Sets feature.
  - **Downloadable ACLs**—Allows the administrator full access to the Downloadable PIX ACLs feature.
  - **Create New Device Command Set Type**—Allows the administrator account to be used as valid credentials by another Cisco application for adding new device command set types. New device command set types that are added to Cisco Secure ACS using this privilege appear in the Shared Profile Components section of the HTML interface.
  - **Shell Command Authorization Sets**—Allows the administrator full access to the Shell Command Authorization Sets feature.
  - **PIX Command Authorization Sets**—Allows the administrator full access to the PIX Command Authorization Sets feature.

Note Additional command authorization set privilege options may appear, if other Cisco network management applications, such as CiscoWorks2000, have updated the configuration of Cisco Secure ACS.

- **Network Configuration**—Allows the administrator full access to the features in the Network Configuration section of the HTML interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 341
3698
Doc.

- **System Configuration...**—Contains the privilege options for the features found in the System Configuration section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **Service Control**—For more information about this feature, see Service Control, page 8-2.
  - **Date/Time Format Control**—For more information about this feature, see Date Format Control, page 8-3.
  - **Logging Control**—For more information about this feature, see Logging, page 8-3.
  - **Local Password Management**—For more information about this feature, see Local Password Management, page 8-5.
  - **DB Replication**—For more information about this feature, see CiscoSecure Database Replication, page 9-1.
  - **RDBMS Synchronization**—For more information about this feature, see RDBMS Synchronization, page 9-23.
  - **IP Pool Address Recovery**—For more information about this feature, see IP Pools Address Recovery, page 9-44.
  - **IP Pool Server Configuration**—For more information about this feature, see IP Pools Server, page 9-37.
  - **ACS Backup**—For more information about this feature, see Cisco Secure ACS Backup, page 8-8.
  - **ACS Restore**—For more information about this feature, see Cisco Secure ACS System Restore, page 8-13.
  - **ACS Service Management**—For more information about this feature, see Cisco Secure ACS Active Service Management, page 8-17.
  - **VoIP Accounting Configuration**—For more information about this feature, see VoIP Accounting Configuration, page 8-21.
  - **ACS Certificate Setup**—For more information about this feature, see Cisco Secure ACS Certificate Setup, page 10-15.
  - **Global Authentication Setup**—For more information about this feature, see Global Authentication Setup, page 10-11.
  - **Appliance Configuration**—For more information about this feature, see Appliance Configuration, page 8-22.

- **Support Operations**—For more information about this feature, see Support, page 8-24.
- **View Diagnostic Logs**—For more information about this feature, see Viewing or Downloading Diagnostic Logs, page 8-27.
- **Appliance Upgrade Status**—For more information about this feature, see Viewing or Downloading Diagnostic Logs, page 8-27.

- **Interface Configuration**—Allows the administrator full access to the features in the Interface Configuration section of the HTML interface.
- **Administration Control**—Allows the administrator full access to the features in the Administration Control section of the HTML interface.
- **External User Databases**—Allows the administrator full access to the features in the External User Databases section of the HTML interface.
- **Reports & Activity**—Contains the privilege options for the reports and features found in the Reports and Activity section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **TACACS+ Accounting**—For more information about this report, see Accounting Logs, page 11-5.
  - **TACACS+ Administration**—For more information about this report, see Accounting Logs, page 11-5.
  - **RADIUS Accounting**—For more information about this report, see Accounting Logs, page 11-5.
  - **VoIP Accounting**—For more information about this report, see Accounting Logs, page 11-5.
  - **Passed Authentications**—For more information about this report, see Accounting Logs, page 11-5.
  - **Failed Attempts**—For more information about this report, see Accounting Logs, page 11-5.
  - **Logged-in Users**—For more information about this report, see Accounting Logs, page 11-5.
  - **Purge of Logged-in Users**—For more information about this feature, see Deleting Logged-in Users, page 11-9.
  - **Disabled Accounts**—For more information about this report, see Deleting Logged-in Users, page 11-9.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 342
Doc. 3698

- **ACS Backup and Restore**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **DB Replication**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **RDBMS Synchronization**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **Administration Audit**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **ACS Service Monitor**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **User Change Password**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **Appliance Status**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **Appliance Administration Audit**—For more information about this report, see Deleting Logged-in Users, page 11-9.

Adding an Administrator Account

Before You Begin

For descriptions of the options available while adding an administrator account, see Administrator Privileges, page 12-2.

To add a Cisco Secure ACS administrator account, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Step 2 Click **Add Administrator**.

Result: The Add Administrator page appears.

Step 3 Complete the boxes in the Administrator Details table:

a. In the Administrator Name box, type the login name (up to 32 characters) for the new Cisco Secure ACS administrator account.

8188
A-

b. In the Password box, type the password (up to 32 characters) for the new Cisco Secure ACS administrator account.

c. In the Confirm Password box, type the password a second time.

Step 4 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

Result: All privilege options are selected. All user groups move to the Editable groups list.

Tip To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Step 5 To grant user and user group editing privileges, follow these steps:

a. Select the desired check boxes under User & Group Setup.

b. To move a user group to the Editable groups list, select the group in the Available groups list, and then click —> (right arrow button).

Result: The selected group moves to the Editable groups list.

c. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <— (left arrow button).

Result: The selected group moves to the Available groups list.

d. To move all user groups to the Editable groups list, click >>.

Result: The user groups in the Available groups list move to the Editable groups list.

e. To remove all user groups from the Editable groups list, click <<.

Result: The user groups in the Editable groups list move to the Available groups list.

Step 6 To grant any of the remaining privilege options, in the Administrator Privileges table, select the applicable check boxes.

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 343
Doc. 3698

Editing an Administrator Account

You can edit a Cisco Secure ACS administrator account to change the privileges granted to the administrator. You can effectively disable an administrator account by revoking all privileges.

Note You cannot change the name of an administrator account; however, you can delete an administrator account and then create an account with the new name. For information about deleting an administrator account, see Deleting an Administrator Account, page 12-11. For information about creating an administrator account, see Adding an Administrator Account, page 12-6.

For information about administrator privilege options, see Administrator Privileges, page 12-2.

Before You Begin

For descriptions of the options available while editing an administrator account, see Administrator Privileges, page 12-2.

To edit Cisco Secure ACS administrator account privileges, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose privileges you want to edit.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

Step 3 To change the administrator password, follow these steps:

a. In the Password box, double-click the asterisks, and then type the new password (up to 32 characters) for the administrator.

Result: The new password replaces the existing, masked password.

b. In the Confirm Password box, double-click the asterisks, and then type the new administrator password a second time.

Result: The new password is effective immediately after you click Submit in Step 9.

8186
A.

Step 4 If the Reset current failed attempts count check box appears below the Confirm Password box and you want to allow the administrator whose account you are editing to access the Cisco Secure ACS HTML interface, select the **Reset current failed attempts count** check box.

Note If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator cannot access Cisco Secure ACS unless you complete Step 4. For more information about re-enabling an administrator account, see Unlocking a Locked Out Administrator Account, page 12-10.

Step 5 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

Result: All privilege options are selected. All user groups move to the Editable groups list.

Step 6 To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Result: All privileges options are cleared. All user groups move to the Available groups list.

Step 7 To grant user and user group editing privileges, follow these steps:

a. Under User & Group Setup, select the applicable check boxes.

b. To move all user groups to the Editable groups list, click >>.

Result: The user groups in the Available groups list move to the Editable groups list.

c. To move a user group to the Editable groups list, select the group in the Available groups list, and then click —> (right arrow button).

Result: The selected group moves to the Editable groups list.

d. To remove all user groups from the Editable groups list, click <<.

Result: The user groups in the Editable groups list move to the Available groups list.

e. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <— (left arrow button).

Result: The selected group moves to the Available groups list.

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 341
Doc. 3608

Step 8 To grant any remaining privilege options, select the applicable check boxes in the Administrator Privileges table.

Step 9 To revoke any remaining privilege options, clear the applicable check boxes in the Administrator Privileges table.

Step 10 Click **Submit**.

Result: Cisco Secure ACS saves the changes to the administrator account.

Unlocking a Locked Out Administrator Account

Cisco Secure ACS disables the accounts of administrators who have attempted to access the Cisco Secure ACS HTML interface and have provided an incorrect password in more successive attempts than is specified on the Session Policy Setup page. Until the failed attempts counter for a disabled administrator account is reset, the administrator cannot access the HTML interface.

For more information about configuring how many successive failed login attempts can occur before Cisco Secure ACS disables an administrator account, see Session Policy, page 12-16.

To reset the failed attempts count for an administrator, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose account you want to re-enable.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator account cannot access the HTML interface.

Step 3 Select the **Reset current failed attempts count** check box.

Step 4 Click **Submit**.

Result: Cisco Secure ACS saves the changes to the administrator account.

Deleting an Administrator Account

You can delete a Cisco Secure ACS administrator account when you no longer need it. We recommend deleting any unused administrator accounts.

To delete a Cisco Secure ACS administrator account, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 In the Administrators table, click the name of the administrator account that you want to delete.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

Step 3 Click **Delete**.

Result: Cisco Secure ACS displays a confirmation dialog box.

Step 4 Click **OK**.

Result: Cisco Secure ACS deletes the administrator account. The Administrators table on the Administration Control page no longer lists the administrator account that you deleted.

Access Policy

The Access Policy feature affects access to the Cisco Secure ACS HTML interface. You can limit access by IP address and by the TCP port range used for administrative sessions. You can also enable secure socket layer (SSL) for access to the HTML interface.

This section contains the following topics:

- Access Policy Options, page 12-12
- Setting Up Session Policy, page 12-16

Access Policy Options

You can configure the following options on the Access Policy Setup page:

- **IP Address Filtering**—Contains the following IP address filtering options:
  - **Allow all IP addresses to connect**—Allow access to the HTML interface from any IP address.
  - **Allow only listed IP addresses to connect**—Allow access to the HTML interface only from IP addresses *inside* the address range(s) specified in the IP Address Ranges table.
  - **Reject connections from listed IP addresses**—Allow access to the HTML interface only from IP addresses *outside* the address range(s) specified in the IP Address Ranges table.
- **IP Address Ranges**—The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the start and end IP addresses. The IP addresses entered to define a range must differ only in the last octet (Class C format).

  The IP Address Ranges table contains one column of each of the following boxes:
  - **Start IP Address**—Defines the lowest IP address of the range specified in the current row.
  - **End IP Address**—Defines the highest IP address of the range specified in the current row.
- **HTTP Port Allocation**—Contains the following options for configuring TCP ports used for remote access to the HTML interface.
  - **Allow any TCP ports to be used for Administration HTTP Access**—Allow the ports used by administrative HTTP sessions to include the full range of TCP ports.
  - **Restrict Administration Sessions to the following port range From Port *X* to Port *Y***—Restrict the ports used by administrative HTTP sessions to the range specified in the *X* and *Y* boxes, inclusive. The size of the range specified determines the maximum number of concurrent administrative sessions.

Cisco Secure ACS uses port 2002 to start all administrative sessions. You do not need to include port 2002 in the port range. Also, Cisco Secure ACS does not allow you to define an HTTP port range that consists only of port 2002. Your port range must consist of at least one port other than port 2002.

A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a web browser must address to initiate an administrative session.

Note We do not recommend allowing administration of Cisco Secure ACS from outside a firewall. If you do choose to allow access to the HTML interface from outside a firewall, keep the HTTP port range as narrow as possible. This can help prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or "spoof," the IP address of a legitimate host to make use of the active administrative session HTTP port.

- **Secure Socket Layer Setup**—The Use HTTPS Transport for Administration Access check box defines whether Cisco Secure ACS uses secure socket layer protocol to encrypt HTTP traffic between the CSAdmin service and a web browser used to access the HTML interface. When this option is enabled, all HTTP traffic between the browser and Cisco Secure ACS is encrypted, as reflected by the URLs, which begin with HTTPS. Additionally, most browsers include an indicator for when a connection is SSL-encrypted.

  To enable SSL, you must have completed the steps in Installing a Cisco Secure ACS Certificate, page 10-15 and Adding a Certificate Authority Certificate, page 10-18.

Setting Up Access Policy

For information about access policy options, see Access Policy Options, page 12-12.

CPMI - CORREIOS
Fls. Nº 346
Doc. 3698

Before You Begin

If you want to enable SSL for administrative access, before completing this procedure, you must have completed the steps in Installing a Cisco Secure ACS Certificate, page 10-15 and Adding a Certificate Authority Certificate, page 10-18.

To set up Cisco Secure ACS Access Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Access Policy**.

Result: The Access Policy Setup page appears.

Step 3 To allow remote access to the HTML interface from any IP address, in the IP Address Filtering table, select the **Allow all IP addresses to connect** option.

Step 4 To allow remote access to the HTML interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Allow only listed IP addresses to connect** option.

b. For each IP address range from within which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. In the Start IP Address box, type the lowest IP address (up to 16 characters) in the range. In the End IP Address box, type the highest IP address (up to 16 characters) in the range. Use dotted decimal format.

Note The IP addresses entered to define a range must differ only in the last octet.

Step 5 To allow remote access to the HTML interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Reject connections from listed IP addresses** option.

b. For each IP address range from outside which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. Type the lowest IP address (up to 16 characters) in the range in the Start IP Address box. Type the highest IP address (up to 16 characters) in the range in the End IP Address box.

Note The IP addresses entered to define a range must differ only in the last octet.

Step 6 If you want to allow Cisco Secure ACS to use any valid TCP port for administrative sessions, under HTTP Port Allocation, select the **Allow any TCP ports to be used for Administration HTTP Access** option.

Step 7 If you want to allow Cisco Secure ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:

a. Under HTTP Port Allocation, select the **Restrict Administration Sessions to the following port range From Port** *X* **to Port** *Y* option.

b. In the *X* box type the lowest TCP port (up to 5 characters) in the range.

c. In the *Y* box type the highest TCP port (up to 5 characters) in the range.

Step 8 If you want to enable SSL encryption of administrator access to the HTML interface, under Secure Socket Layer Setup, select the **Use HTTPS Transport for Administration Access** check box.

Note To enable SSL, you must have completed the steps in Installing a Cisco Secure ACS Certificate, page 10-15 and Adding a Certificate Authority Certificate, page 10-18.

Step 9 Click **Submit**.

Result: Cisco Secure ACS saves and begins enforcing the access policy settings.

If you have enabled SSL, at the next administrator login, Cisco Secure ACS begins using HTTPS. Any current administrator sessions are unaffected.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 347
Doc. 3698

Session Policy

The Session Policy feature controls various aspects of Cisco Secure ACS administrative sessions. This section contains the following topics:

- Session Policy Options, page 12-16
- Setting Up Session Policy, page 12-16

Session Policy Options

You can configure the following options on the Session Policy Setup page:

- **Session idle timeout (minutes)**—Defines the time in minutes that an administrative session must remain idle before Cisco Secure ACS terminates the connection. This parameter applies to the Cisco Secure ACS administrative session in the browser only. It does not apply to an administrator dial-up session.

  An administrator whose administrative session is terminated receives a dialog box asking whether or not the administrator wants to continue. If the administrator chooses to continue, Cisco Secure ACS starts a new administrative session.

- **Respond to Invalid IP Address Connections**—Enables an error message in response to attempts to start a remote administrative session using an IP address that is invalid according to the IP address ranges configured in Access Policy. Disabling this option can help prevent unauthorized users from discovering Cisco Secure ACS.

- **Lock out Administrator after *X* successive failed attempts** —Enables Cisco Secure ACS to lock out an administrator after the number of successive failed login attempts specified in the *X* box. A value of 0 (zero) in the X box allows unlimited successive administrative login failures. If this check box is selected, the X box cannot be set to zero.

Setting Up Session Policy

For information about session policy options, see Session Policy Options, page 12-16.

To setup Cisco Secure ACS Session Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Session Policy**.

Result: The Session Policy Setup page appears.

Step 3 To define the number of minutes of inactivity after which Cisco Secure ACS ends an administrative session, in the Session idle timeout (minutes) box, type the number of minutes (up to 4 characters).

Step 4 Set the invalid IP address response policy:

a. To configure Cisco Secure ACS to respond with a message when an administrative session is requested from an invalid IP address, select the **Respond to invalid IP address connections** check box.

b. To configure Cisco Secure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** check box.

Step 5 Set the failed administrative login attempts policy:

a. To enable Cisco Secure ACS to lock out an administrator after a number of successive failed administrative login attempts, select the **Lock out Administrator after *X* successive failed attempts** check box.

b. In the *X* box, type the number of successive failed login attempts after which Cisco Secure ACS locks out an administrator. The *X* box accepts up to 4 characters.

Step 6 Click **Submit**.

Result: Cisco Secure ACS saves and begins enforcing the session policy settings you made.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 348
3698
Doc.

Apêndice HT

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 349
Doc. 3698

8376
A

Cisco Systems

Data Sheet

Cisco Secure **Access Control Server** Solution Engine

The Cisco® Secure Access Control Server (ACS) provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure. The Cisco Secure ACS Solution Engine adds new security improvements, simplified management, and reduced total cost of ownership (TCO) for the operation of the underlying ACS service.

Introduction

The Cisco Secure ACS Solution Engine is a high-performance and highly scalable user and administrative access control solution that operates as a centralized RADIUS or TACACS+ server system for the Cisco 1111 platform. Packaged in a dedicated and secure 1-rack-unit (1-RU) hardened appliance, the Cisco Secure ACS Solution Engine provides a reduced-configuration, plug and play solution, and highly reliable platform with the unique ability to protect existing networking infrastructure through fully Web-based remote-access and configuration capabilities.

The need for security appliances is rapidly increasing in today's IT space. Security, convenience, and ease of installation and troubleshooting are the important advantages of security appliances compared to the many software-based security applications that exist in the marketplace today. The innovative, new, 1-RU, security-hardened Cisco Secure ACS Solution Engine was designed to specifically alleviate the security issue with a closed-device design that makes it substantially more difficult for intruders to penetrate than an open-platform system.

Security appliances provide an all-in-one approach that simplifies product selection, product integration, and ongoing support. By combining all necessary operating system installation and patching with the ACS software service, customers can avoid maintaining software versioning and proliferation of servers, patches, and operating system (OS) maintenance issues. This is particularly important in large networking environments where security solutions are required in remote sites with no IT professionals present to regularly manage and upgrade these solutions. In addition, a security appliance greatly simplifies support and troubleshooting in failure modes, hence enabling quick service restoration (through a one-stop support contact)—an important consideration, especially when the security application is mission-critical, a situation that is true with security authentication, authorization, and accounting (AAA) applications.

Changing network dynamics and increased security threats have influenced new opportunities in access control management solutions. As AAA becomes more relevant and the requirement to

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 350
Doc.

control user access expands beyond just dialup, new trends (including expanded authentication, tracking, and audit management) are emerging that require identity-networking solutions to be pervasive, scalable, and available throughout the network.

Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized location, allowing for greater flexibility and mobility, increased security, and user productivity gains. As an accounting service, the Cisco Secure ACS Solution Engine reduces IT operations costs by providing detailed reporting and monitoring capabilities of network users' behavior and by keeping a record of every access connection and device configuration change across the entire network.

Cisco Secure ACS provides a centralized identity networking solution and simplified user-management experience across all Cisco devices and security-management applications. Cisco Secure ACS ensures enforcement of assigned policies by allowing network administrators to control:

- Who can log in to the network
- What privileges each user has in the network
- What accounting information is recorded in terms of security audits or account billing
- What access and command controls are enabled for each configuration administrator

Like the Cisco Secure ACS for Windows, the Cisco Secure ACS Solution Engine supports a wide array of access connection types, including wired or wireless LAN, dialup, broadband, content, storage, voice over-IP (VoIP), firewall, and virtual private networks (VPNs).

Cisco Secure ACS Solution Engine Highlights

The Cisco Secure ACS Solution Engine is a highly secure, OS-independent, and dedicated platform that offers a highly manageable access control solution with an increasingly reduced setup and troubleshooting time. The Cisco Secure ACS Solution Engine provides Plug and Play deployment, a highly reliable AAA solution, and increased TCO protection through the high availability and simplified day-to-day operation and management of the Cisco Secure ACS service. It provides the same features and functions as the Cisco Secure ACS for Windows, in a dedicated, security-hardened, application-specific appliance package. Customers with existing Windows-based Cisco Secure ACS deployments can add or upgrade to Cisco Secure ACS Solution Engines without any effect on existing AAA configurations, including remote logging and replication configurations. More information about the latest Cisco Secure ACS features is available from the Cisco Secure ACS for Windows data sheet.

To ensure the high-security posture of the Cisco Secure ACS Solution Engine, additional functions specific to operating and managing the Cisco Secure ACS Solution Engine are provided. Additionally, a Cisco Secure ACS remote agent is available with each Cisco Secure ACS Solution Engine to enable remote logging and Windows authentication. Forwarding all accounting data from the solution engine to a remote agent preserves disk space on the solution engine. It also improves AAA performance by eliminating the frequent and time-consuming disk writes required for local logging on the solution engine. Also, because a Cisco Secure ACS Solution Engine is never a member of a Microsoft Windows domain, the Cisco Secure ACS remote agent establishes the necessary Windows domain trust relationships for Windows-based authentication.

Table 1 lists additional functions provided by the Cisco Secure ACS Solution Engine. These functions are not available from the Cisco Secure ACS for Windows software product.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8174
A.

Table 1 Functions Provided by the Cisco Secure ACS Solution Engine

Hardened underlying operating system	• The Cisco Secure ACS Solution Engine is dedicated to run only the Cisco Secure ACS service, thereby preventing any appliance-based OS changes, additions, or configuration modifications.
Serial console interface	• A serial console interface is provided on the Cisco Secure ACS Solution Engine for initial configuration, subsequent management of IP connections, access to the Cisco Secure ACS HTML interface, and application of upgrade and recovery procedures. • The serial console interface supports both serial line and Telnet connections through which the Cisco Secure ACS service can be reimaged, reloaded, and rebooted, both locally and remotely.
Solution Engine-specific management tools	• Integrated into the existing Cisco Secure ACS HTML interface, Solution Engine-specific management tools provide generic appliance-management capabilities, including backup, recovery, software upgrades, monitoring, maintenance, and troubleshooting functions. • The Cisco Secure ACS HTML interface is accessed though a secured Secure Sockets Layer (SSL)-based connection.
Cisco Secure ACS remote agent	• The Cisco Secure ACS remote agent provides two functions: authentication against Windows domains and remote logging capabilities of user accounting records. • Administrators can provision primary and backup Cisco Secure ACS remote agents in distributed Cisco Secure ACS configurations.
Port-based packet filtering	• The Cisco Secure ACS Solution Engine implements a packet-filtering service to block traffic on all but the necessary Cisco Secure ACS-specific TCP and UDP ports.
Network Timing Protocol (NTP) support	• The Cisco Secure ACS Solution Engine has built-in NTP functions to maintain network timing synchronization and consistency with other Cisco Secure ACS appliances or network devices.

Cisco Secure ACS Solution Engine-Specific Benefits

In addition to the many benefits the Cisco Secure ACS solution brings in controlling user and administrative AAA inside your network, the Cisco Secure ACS Solution Engine, with its 1-RU hardened form factor, adds specific security and operational advantages in the following areas:

- *Security*—With a security-hardened service focused on running exclusively the Cisco Secure ACS service, the solution engine significantly increases the security posture of the Cisco Secure ACS system. All solution engine services and ports not used by the Cisco Secure ACS service are disabled to secure access to the Cisco Secure ACS Solution Engine.
- *Plug and Play solution*—The Cisco Secure ACS Solution Engine provides a record service uptime before starting to configure the Cisco Secure ACS service.
- *Manageability*—With a dedicated, exclusive, and complete Cisco Secure ACS solution, the appliance greatly simplifies manageability and support of the Cisco Secure ACS service while removing the necessity to manage any UNIX or Windows network operating systems.
- *Supportability*—With no external services or applications (other than the Cisco Secure ACS service) allowed to be installed on the solution engine, the support and the day-to-day management of the Cisco Secure ACS Solution Engine are greatly simplified.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 351
3698
Doc.

- *Reliability*—Enabling only the services that are required by Cisco Secure ACS allows an increase in overall reliability and security of the Cisco Secure ACS service.
- *TCO*—With a turnkey security-hardened solution engine that is easily deployed, Cisco is able to guarantee full support, maintenance, and serviceability of the overall Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations, supported by third-party vendors.
- *Migration from Cisco Secure ACS UNIX*—The Cisco Secure ACS Solution Engine provides a suitable alternative for Cisco Secure ACS UNIX customers not willing to install or manage Cisco Secure ACS on the Windows OS.

System Requirements

Hardware Requirements

The Cisco Secure ACS Solution Engine is available on Cisco 1111 platforms with the following specifications:

- Pentium IV processor, 2.66 GHz
- 1 GB RAM
- 40 GB free disk space
- Two built-in 10/100 Ethernet controllers
- 1 floppy disk drive
- 1 CD-ROM drive

The Cisco Secure ACS remote agent is available in a Windows version that can be installed on a Windows 2000 Server (Windows Domain Controller or Member Server supported).

The computer running Cisco Secure ACS remote agent for Windows must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster
- 256 MB RAM
- 250 MB free disk space

Ordering Information

The Cisco Secure ACS Solution Engine is available for purchase through normal Cisco sales and distribution channels worldwide. The Cisco Secure ACS Solution Engine is shipped with a preinstalled Cisco Secure ACS Software license.

For More Information

For more information about Cisco Secure ACS, visit: http://www.cisco.com/go/acs.

For specific product functions or technical questions, send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

For questions about product ordering, availability, and support contract information, send e-mail to the product marketing group at ciscoworks@cisco.com.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8172
A-

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, Catalyst, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 352
Doc. 3608

Apêndice HU

RQS nº 03/2005 - C
CPMI - CORREIOS
Fls. Nº 3543
Doc 3698

Cisco Systems

8171
A-

Q & A

Cisco Secure **Access Control Server** Solution Engine

Q. What is Cisco® Secure Access Control Server (ACS) Solution Engine?

A. Cisco Secure ACS Solution Engine is a highly scalable, one-rack-unit (RU), dedicated platform that serves as a high-performance access control server supporting centralized Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+). Cisco Secure ACS Solution Engine controls the authentication, authorization, and accounting (AAA) for users accessing corporate resources through the network.

Q. What does Cisco Secure ACS Solution Engine do?

A. Cisco Secure ACS Solution Engine enables you to control who can access the network, to authorize what types of network services are available for users or groups of users, and to keep an accounting record of all user actions in the network. The Solution Engine supports access control and accounting for dial-up access servers, firewalls and VPNs, voice-over-IP (VoIP) solutions, content networking, storage networks, and switched and wireless LANs (WLANs). In addition, the AAA framework can be used to manage the administrative roles and groups via TACACS+ and to control how network administrators are able to change, access, and configure the network internally.

Q. Why did Cisco add an Solution Engine to the existing Windows server software packaging for Cisco Secure ACS?

A. The decision to create a dedicated solution engine version of Cisco Secure ACS was made based on several factors:

- Security—The need to create a turnkey security-hardened service focused on running the Cisco Secure ACS service exclusively. The solution engine can remove all extraneous services, block all unused ports, and otherwise prevent all other access to the Cisco Secure ACS server system—dramatically increasing the security posture of Cisco Secure ACS.
- Manageability—Cisco Secure ACS Solution Engine is a dedicated, exclusive service for AAA with no ability to install or run other services or applications. This greatly facilitates the support and day-to-day management of the Cisco Secure ACS system.
- Reliability—By targeting only the operating system services required by Cisco Secure ACS, the solution engine offers greater operational reliability and security for the Cisco Secure ACS system.
- Total cost of ownership—Customers choosing Cisco Secure ACS can optimize their total cost of ownership. Cisco end-to-end support now includes

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 354
Doc: 3698

full support, maintenance, and serviceability of the Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations and supported by various third-party vendors.

- Plug and play—Cisco Secure ACS Solution Engine is shipped already installed with Cisco Secure ACS application software, greatly reducing the time it takes to set up and deploy Cisco Secure ACS in your network.
- Migration from Cisco Secure ACS UNIX—Cisco Secure ACS Solution Engine was built and targeted as a suitable migration platform for Cisco Secure ACS for Unix customers not willing to install or manage Cisco Secure ACS on a Windows server.

Q. What are the differences between the Cisco Secure ACS software server and Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine provides the same features and functions of the Cisco Secure ACS Windows version—in a dedicated, security-hardened, application-specific option. The appliance includes features specific to the operation and management of Cisco Secure ACS, and specific software features needed to be customized or removed due to the different underlying system architectures:

Authentication

- Authentication against a Windows domain requires a Cisco Secure ACS remote agent running on a domain controller or member server. The Cisco Secure ACS remote agent is necessary to establish a Windows member or domain controller trust relationship.
- Authentication against an Open Database Connectivity (ODBC) source is not supported. Lightweight Directory Access Protocol (LDAP) authentication can be used instead.
- Authentication against One-Time Password (OTP) directories is performed using the generic RADIUS-based OTP interface on the appliance. Any OTP vendor that provides an RFC-compliant RADIUS interface can interface with Cisco Secure ACS.

User Database Synchronization

- User database synchronization with an ODBC source is not supported. Instead, the administrator can configure Cisco Secure ACS to synchronize its user database with a comma-separated values (CSV) file on a remote File Transfer Protocol (FTP) server.

ODBC Logging

- ODBC logging is not supported. Administrators can use local or remote CSV logging.

Backup/Restore and Appliance Diagnostics

- Backup/restore and gathered appliance diagnostics are performed through a remote FTP server and configured using the current Cisco Secure ACS HTML graphical user interface (GUI).

Q. What additional features are available on Cisco Secure ACS Solution Engine but not available on the Windows version?

A. To ensure the highly secure posture of Cisco Secure ACS Solution Engine, functions specific to operating and managing the appliance have been added:

- Security-hardened underlying operating system.
- Port-based packet filtering, allowing connections only to the ports necessary for Cisco Secure ACS operation.
- Serial console interface for initial configuration, subsequent management of IP connections, Web interface, and application of upgrades and remote reboots. The serial console interface supports both serial line and Telnet connections.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8169
A

- Backup/restore of Cisco Secure ACS data via FTP protocol.
- Recovery procedures.
- NTP (Network Time Protocol) support for maintaining network time consistency with other appliances or network devices.

Q. Are there any additions to the existing Cisco Secure ACS GUI to support Cisco Secure ACS Solution Engine?

A. Yes. New HTML pages specific to Cisco Secure ACS Solution Engine have been added to the Cisco Secure ACS GUI. These pages cover specific features around the operation and management of the solution engine and include:

- Solution Engine configuration page
- Solution Engine remote agent configuration page
- Solution Engine upgrade page
- Solution Engine status page
- Solution Engine diagnostics log view

Q. What ports and protocols access Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine implements a packet filtering service to block the traffic on all but necessary TCP/User Datagram Protocol (UDP) ports. Only the ports listed in Table 1 are open for input traffic:

Table 1 Cisco Secure ACS Solution Engine Ports Usage

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication and authorization (original draft RFC)	1645	
RADIUS accounting (original draft RFC)	1646	
RADIUS authentication and authorization (revised RFC)	1812	
RADIUS accounting (revised draft RFC)	1813	
TACACS+ AAA		49
Replication and RDBMS synchronization		2000
Cisco Secure ACS remote logging		2001
Cisco Secure ACS distributed logging (appliance only)		2003
Hypertext Transfer Protocol (HTTP) administrative access (at login)		2002
Administrative access (after login) port range		Configurable (default 1024-65535)[1]

1. ACS assigns unique port number from the range to each administration session

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 355
3698
Doc.

8168 A

Q. What is the hardware platform specification for Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine is a security-hardened Cisco Secure ACS server in a dedicated 1-RU box with the following configuration:

- Intel ISP 1100 motherboard with a 2.66-GHz Pentium 4 processor
- 1 GB of RAM
- Two built-in 10/100 Ethernet controllers
- 40-GB IDE hard drive
- One floppy drive
- One CD-ROM drive

Q. How does Cisco Secure ACS Solution Engine authenticate to Windows domains?

A. In general, to authenticate Windows NT 4.0 or Active Directory domain users, you must establish a Windows member or domain controller trust relationship. Since Cisco Secure ACS Solution Engine does not run the necessary Windows server services to establish this trust, an external Cisco Secure ACS remote agent is provided with the appliance solution, allowing the trust relationship to be established. The Cisco Secure ACS remote agent can be installed on member servers, domain controllers, or backup domain controllers. NOTE: The best practice is to install the remote agent on a full Domain Controller (DC), as this would allow it to perform its authentication functions with the least extra configuration requirements.

Q. What is the main purpose of the Cisco Secure ACS remote agent?

A. The Cisco Secure ACS remote agent has dual roles—it enables authentication against Windows domains, and it allows remote logging capabilities of user accounting records.

Q. What operating systems can the Cisco Secure ACS remote agent be installed on?

A. The Cisco Secure ACS remote agent can be installed on a Windows 2000 server (Windows Domain Controller or Member Server supported). A Solaris version of Cisco Secure ACS will be provided in the future for Sun Solaris installations. Please refer to the Cisco Secure ACS remote agent installation guide for the exact operating system versions and service packs supported.

Q. Can a Cisco Secure ACS remote agent and Cisco Secure ACS Windows coexist on the same server?

A. No. The Cisco Secure ACS remote agent cannot be installed on a server that already has Cisco Secure ACS Windows installed.

Q. Can a solution engine be configured to use several remote agents?

A. Yes. A solution engine can be configured to use one or more agents. There is no restriction that the same agent be used for Windows services and logging services. For Windows services, an appliance can point to a primary and backup agent, in the event that the primary agent is unavailable.

Q. Can a Cisco Secure ACS remote agent be shared with multiple solution engines?

A. Yes. The Cisco Secure ACS remote agent can be shared with multiple solution engines. There is no hard limit to the number of Cisco Secure ACS solution engines that can share a single remote agent, but Cisco will support configurations with up to five solution engines sharing a single Cisco Secure ACS remote agent. If user accounting records from multiple Cisco Secure ACS solution engines need to be consolidated and centralized, it is desired that all these solution engines share a single Cisco Secure ACS remote agent.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8167
A

Q. Can I perform local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent?

A. Yes. However, local logging on Cisco Secure ACS Solution Engine is constrained in size, forcing log files to be recycled after seven days. The Cisco Secure ACS remote agent provides full, unconstrained logging capability to a remote server.

Q. Are there any differences in the type of Windows databases supported by the Cisco Secure ACS remote agent and the ones supported by Cisco Secure ACS Windows?

A. No. The Cisco Secure ACS remote agent supports the same Windows databases supported by Cisco Secure ACS Windows.

Q. What 802.1X authentication types does the Cisco Secure ACS remote agent support?

A. The Cisco Secure ACS remote agent supports the same 802.1X authentication types available on Cisco Secure ACS for Windows. This includes Extensible Authentication Protocol (EAP)-MD5, EAP-TLS, EAP Cisco Wireless, LEAP, PEAP-EAP-GTC, and PEAP-EAP-MSCHAPv2.

Q. Can a Cisco Secure ACS remote agent be provisioned for Cisco Secure ACS for Windows?

A. No. In its initial release, the Cisco Secure ACS remote agent only operates with Cisco Secure ACS Solution Engine. No communication is possible between a Cisco Secure ACS remote agent and a Cisco Secure ACS service on Windows. However, this limitation does not prevent Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine from operating in the same network environment.

Q. What happens to the standard HTML reports on the solution engine? Do they stay the same?

A. In general, these reports stay the same. The solution engine reports will be constrained in size with no support for multiple rolled over files. The Cisco Secure ACS remote agent will provide full, unconstrained report capability on a remote FTP server.

Q. What happens with third-party software tools, such as backup services from Legato?

A. Cisco Secure ACS Solution Engine is a standalone, dedicated box for running Cisco Secure ACS. There are no interfaces or abilities to add third-party software of any kind to the box. Cisco will investigate third-party extensibility, but at present, nothing can be installed on the Cisco Secure ACS Solution Engine other than Cisco Secure ACS images and patches downloaded via FTP. For Cisco Secure ACS backup, Cisco will create an export file that is automatically exported to an external FTP server. Backup tools can be installed and used to backup the external server.

Q. Can I run Cisco Secure ACS in "mixed mode" (for example, run instances of the Cisco Secure ACS Windows and additional instances of Cisco Secure ACS Solution Engine)?

A. Yes. Cisco will support environments using both Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine.

Q. How is Cisco Secure ACS replication affected with the introduction of Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS replication functions will remain unchanged with the introduction of Cisco Secure ACS Solution Engine. Replication between Cisco Secure ACS Solution Engine and Cisco Secure ACS Windows, as well as replication among Cisco Secure ACS solution engines, will be supported with no impact on any of the solution engines or Windows configurations.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 356
3698
Doc.

8366
A

Q. Are there any restrictions on whether Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be a master database in a replicated configuration?

A. No. Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be the master databases replicating to Cisco Secure ACS Windows slaves, Cisco Secure ACS Solution Engine slaves, or both Windows and solution engine slaves at the same time.

Q. Are there any changes to single logon and password aging capabilities in Cisco Secure ACS Solution Engine?

A. No. With the appropriate Windows or domain controller trust relationships established with the Cisco Secure ACS remote agent, single logon and password aging capabilities remain unchanged from Cisco Secure ACS Windows version.

Q. How scalable is a Cisco Secure ACS Solution Engine?

A. The Cisco Secure ACS Solution Engine follows, as a minimum, the same scalability performance as a Windows-based Cisco Secure ACS server. Cisco Secure ACS guidelines and performance analysis shows that each Cisco Secure ACS server can support anywhere from 20,000 to 80,000 users per server, and can scale to support in excess of 10,000 devices, depending on configuration, platform, and usage scenarios. The real challenge in scaling a user access control framework is on the back end. Linked to a high-performance back-end database such as Oracle or Sybase, Cisco has deployed Cisco Secure ACS for Windows 2000 and NT in clustered deployments into customers with hundreds of thousands of user records.

Q. What Cisco Secure ACS Solution Engine features enhance Cisco Secure ACS reliability and remote management?

A. The operating system is configured to automatically reboot on system crash. The serial console service is configured to automatically restart if it fails. Cisco Secure ACS software implements the monitor that will restart Cisco Secure ACS services if they fail. The solution engine also provides a remote administrator command line interface (CLI). The CLI supports both serial line and Telnet connections, and the Cisco Secure ACS service can be reimaged, reloaded, upgraded, and rebooted remotely from the CLI interface.

Q. What support is there for LDAP?

A. Support for LDAP on the appliance is identical to present support from the Cisco Secure ACS Software version. Cisco Secure ACS supports user authentication against records kept in a directory server through LDAP. Cisco Secure ACS supports the most popular directory servers, including Novell and Netscape LDAP Servers, through a generic LDAP interface.

Q. Will Cisco Secure ACS Solution Engine allow "single login" for Windows networking?

A. Yes. Cisco Secure ACS can be set up so that a user will only need to enter a user name and password once. This is considered a "single login." The Cisco Secure ACS remote agent is required to be installed on a Windows network server with the necessary trust relationships to the domain defined.

Q. Does Cisco Secure ACS support OTP and token systems?

A. Yes. Cisco Secure ACS can be configured to communicate with token solutions from ActiveCard, Cryptocard, PassGo Technologies, RSA Data Security, Secure Computing, and Vasco. Cisco Secure ACS Solution Engine includes a generic RADIUS interface for expanding OTP coverage to new vendors. Any OTP vendor that provides an RFC-compliant RADIUS interface should work with Cisco Secure ACS Solution Engine.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8105
A.

Q. What's new in Cisco Secure ACS Version 3.2 for access control functions and features?

A. Cisco Secure ACS Version 3.2 is a minor update to Cisco Secure ACS Version 3.1. It adds the following main features:

- Cisco Secure ACS Solution Engine support
- EAP-MSCHAPv2 support within the Protected EAP (PEAP) framework (used for both wireless and wired environments)
- Machine-based authentication (through EAP-TLS and EAP-MSCHAPv2)
- PEAP authentication against the internal Cisco Secure ACS database
- EAP-TLS authentication against ODBC databases
- EAP-TLS session resume support
- Accounting support for Cisco Aironet® clients
- LDAP multithreading
- Downloadable access control lists (ACLs) for VPN solutions

Please refer to the Cisco Secure ACS Version 3.2 data sheet for more information about the features and functions introduced in this release.

Q. How is Cisco Secure ACS Solution Engine Version 3.2 licensed?

A. Cisco Secure ACS Solution Engine is licensed per server, with unlimited ports, users, and network access servers. The following solution engine packages will be available for ordering. For exact part numbers, refer to the Cisco Secure ACS Version 3.2 product bulletin at: http://www.cisco.com/go/acs

- Cisco Secure ACS Solution Engine Version 3.2
- Cisco Secure ACS Solution Engine upgrade package—Used for upgrading from software versions of Cisco Secure ACS 3.x or Cisco Secure ACS for UNIX to Cisco Secure ACS Solution Engine Version 3.2

Note: The Cisco Secure ACS Solution Engine upgrade package can be ordered when customers have deployed Cisco Secure ACS for Windows or Cisco Secure ACS for UNIX in their networks and want to upgrade to the solution engine version. Please refer to the Cisco Secure ACS Solution Engine user guide and release notes for supported upgrade paths. Current Cisco Secure ACS software maintenance entitlements do not provide a free upgrade to the Cisco Secure ACS Solution Engine.

Q. Can I upgrade to Cisco Secure ACS Version 3.2 from older software versions of Cisco Secure ACS?

A. Yes. A detailed upgrade procedure will be available to guide you through the required steps to complete an upgrade to Cisco Secure ACS Solution Engine. Please refer to the Cisco Secure ACS Solution Engine user guide for more information about the supported upgrade procedure.

Q. Can I purchase or license a backup solution engine?

A. No. An additional Cisco Secure ACS Solution Engine must be purchased as a separate Cisco Secure ACS server license to be used for recovery and backup purposes. Cisco Secure ACS servers can be run as recovery or failover servers. Because Cisco Secure ACS is a central control service in your network, Cisco highly recommends that customers configure a backup server for failover and recovery.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 357
3698
Doc.

8164 A.

Q. Does Cisco Secure ACS Solution Engine operating system need to be updated when upgrading the Cisco Secure ACS firmware?

A. No. Future Cisco Secure ACS image upgrades are applied to Cisco Secure ACS Solution Engine without updating or modifying the underlying Cisco Secure ACS Solution Engine operating system.

Q. Do I need to patch the solution engine with newer operating system releases or patches?

A. No. All operating system software updates and patches are handled by Cisco Secure ACS Solution Engine upgrades performed by Cisco. Any operating system patch that requires changes to Cisco Secure ACS Solution Engine will be provided in a new upgrade/patch.

Q. Can Cisco Secure ACS Solution Engine software be upgraded remotely from a CD-ROM?

A. Yes. Cisco Secure ACS Solution Engine supports remote upgrades from CD-ROM without any FTP server posting requirements.

Q. Can Cisco Secure ACS Solution Engine support software image rollback during patch update verification?

A. Yes. Cisco Secure ACS Solution Engine can roll back to previously installed software when a software patch has been applied. This capability is used for debugging and verification purposes.

Q. What is the status of Cisco Secure ACS for UNIX?

A. Cisco Secure ACS for UNIX is expected to be discontinued, at which point an end-of-life, end-of-sale (EOL/EOS) announcement will be made. Cisco will support all existing customers and provide smooth migration paths as the new platforms become available. The EOL/EOS date has not been determined, but Cisco will provide customer support for Cisco Secure ACS for UNIX customers for a period no shorter than 24 months after the EOL/EOS date. At present, no new features or releases are planned for Cisco Secure ACS for UNIX and only critical, Priority 1 bugs will be addressed.

Q. Can I use my current Cisco Secure ACS Windows maintenance contract to get support on Cisco Secure ACS Solution Engine?

A. No. Separate hardware and software contracts need to be purchased for maintenance support on Cisco Secure ACS Solution Engine. Please refer to refer to the Cisco Secure ACS Version 3.2 product bulletin for more information. http:// www.cisco.com/go/acs

Q. How can I obtain a demo of Cisco Secure ACS Solution Engine?

A. Please contact your Cisco account manager, who will be able to arrange for a limited time demo of Cisco Secure ACS Solution Engine.

Q. Where can I find more information on Cisco Secure ACS?

A. For additional product information, visit: http://www.cisco.com/go/acs

For additional information or questions, please send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

8163
A.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Aironet are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203051/ETMG 05/03

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 358
Doc. 3698

Apêndice HV

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 359
Doc. 3698

8162
A.

Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Appliance version 3.2

Revised: July 8, 2003

Because the number of devices that Cisco Secure ACS Appliance version 3.2 interoperates with runs into the hundreds, this device list differs significantly from those of other Cisco products with which you may be familiar. This document lists supported devices and software, that is, those that we have tested against. However, this document also lists devices and software programs that are, to the best of our knowledge, interoperable. Of the hundreds of devices and software programs that Cisco Secure ACS Appliance version 3.2 interoperates with, Cisco officially supports only those that have been tested.

For details regarding other limitations and known problems see *Release Notes for CiscoSecure Access Control Server Appliance Version 3.2*. On Cisco.com, you can find the latest version all documentation by selecting **Products & Services > Security and VPN Software > Cisco Secure Access Control Server Appliance > Technical Documentation**.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 360
3698
Doc.

With regard to third-party RADIUS and TACACS+ clients, Cisco Secure ACS Appliance fully interoperates with devices that adhere to the governing protocols. Also, support for RADIUS and TACACS+ functions depends on device-specific implementation. On a given device, TACACS+ may not be available for user authentication and authorization. Likewise, RADIUS may not be available for administrative authentication and authorization.

For RADIUS these include the following RFCs:

- RFC 2138 - Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 - RADIUS Accounting
- RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 - RADIUS Accounting
- RFC 2867 - RADIUS Accounting for Tunnel Protocol Support
- RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 - RADIUS Extensions

For details regarding the implementation of vendor-specific attributes (VSAs), see *User Guide for Cisco Secure ACS Appliance Version 3.2*.

Cisco Secure ACS Appliance conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77.

The following tables show the devices and software that Cisco Secure ACS Appliance supports or with which it interoperates:

- Table 1, Web Browsers
- Table 2, Device Operating Systems
- Table 3, Routers
- Table 4, Access Devices/Universal Gateways
- Table 5, Cable Devices
- Table 6, Content Networking Devices
- Table 7, Security and VPN Devices
- Table 8, Storage Networking Devices
- Table 9, Switches
- Table 10, Cisco Aironet Software (Access Points for Wireless LAN)
- Table 11, CiscoWorks VMS

- Table 12, PKI/Certificate Servers
- Table 13, Token Servers
- Table 14, LDAP Servers
- Table 15, User Databases
- Table 16, Proxy Support

You can find information about new device support at Cisco.com, http://www.cisco.com.

To ensure full capabilities, the clients you deploy to interoperate with Cisco Secure ACS Appliance should use the most recent operating systems available. Nonetheless, Table 2 provides details on the minimum acceptable client operating system versions.

Table 1 Web Browsers[1]

Program	Versions	Notes
Microsoft Internet Explorer	5.5 for Microsoft Windows - English Language version	Tested
	6.0 for Microsoft Windows - English Language version	Tested
Netscape	7.0 for Microsoft Windows - English Language version	Tested
	7.0 on Solaris 2.7- English Language version	Tested

1. To use a web browser to access the Cisco Secure ACS HTML interface, you must enable both Java and JavaScript in the browser. Also, the web browser must not be configured to use a proxy server.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 361
Doc.

Table 2 Device Operating Systems

Operating System	Minimum Version	Notes
IOS	11.2	For full RADIUS support
CAT OS	7.2	Cisco products—and other third-party products that are RFC compliant—will work with Cisco Secure ACS even when running earlier versions of CAT OS. However, full functionality, including the 802.1x VLAN assignment, is supported only when the listed version is used.

Table 3 Routers

Series	Notes
Cisco 1400	End of life (EOL) status
Cisco 1600	RADIUS and TACACS+ interoperability
Cisco 1700	Tested with IOS 12.2(8) RADIUS and TACACS+ interoperability
Cisco 2500	EOL status
Cisco 2600	RADIUS and TACACS+ interoperability
Cisco 3600	RADIUS and TACACS+ interoperability
Cisco 3700	Tested with IOS 12.2 RADIUS and TACACS+ interoperability
Cisco 7100	RADIUS and TACACS+ interoperability
Cisco 7200	Tested with IOS 12.2 RADIUS and TACACS+ interoperability
Cisco 7300	RADIUS and TACACS+ interoperability
Cisco7400	RADIUS and TACACS+ interoperability
Cisco 7500	RADIUS and TACACS+ interoperability

Table 3 Routers (continued)

Cisco 10000	RADIUS interoperability
Cisco 10720	RADIUS and TACACS+ interoperability

Table 4 Access Devices/Universal Gateways

Series	Notes
6400 Series	RADIUS and TACACS+ interoperability
AS5350 Series	RADIUS and TACACS+ interoperability
5400 Series	Tested with IOS12.2(7c) RADIUS and TACACS+ interoperability
AS5850 Series	RADIUS and TACACS+ interoperability
DSL Series / 6015, 6100, 6130, 6160, 6260	RADIUS and TACACS+ interoperability
MGX Series / 8220, 8250, 8800, 8950	TACACS+ interoperability

Table 5 Cable Devices

Devices	Notes
uBR7100	Tested with IOS 12.2BC RADIUS and TACACS+ interoperability
uBR7200	EOL status TACACS+ interoperability

Table 6 Content Networking Devices

Series / Devices	Notes
CE7300 / CE 7320	Tested with ACNS 4.2 RADIUS and TACACS+ interoperability

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 362
369
Doc.

Table 6 Content Networking Devices (continued)

Series / Devices	Notes
CDM4600 / CDM4630, CDM4650	RADIUS and TACACS+ interoperability
4400 Content Routers/ CR4430	Tested with ACNS 4.2 RADIUS and TACACS+ interoperability

Table 7 Security and VPN Devices

Series / Devices	Notes
3000 Series Concentrator / 3005, 3015, 3030, 3060, 3080	Tested with 3015 RADIUS and TACACS+ interoperability
PIX 500 Series Firewall / 501, 506E, 515, 515E, 525, 535	Tested with 515 and PIX OS v6.3 RADIUS and TACACS+ interoperability
5000 Series Concentrator	EOL status

Table 8 Storage Networking Devices

Series	Devices Supported	Notes
MDS 9000	MDS 9216, MDS9509	RADIUS interoperability (TACACS+ support in future release)

Table 9 Switches

Series / Devices	Notes
Catalyst 2950/3550	Tested with 3550 and IOS 12.1(12)EA1 RADIUS and TACACS+ interoperability
Catalyst 4000/4500	Tested with Cat4503, CatOS 7.5, and IOS 12.1 RADIUS and TACACS+ interoperability

Table 9 Switches (continued)

Series / Devices	Notes
Catalyst 5000	EOL status
Catalyst 6500	Tested with CatOS 7.5, and IOS 12.1 RADIUS and TACACS+ interoperability

Table 10 Cisco Aironet Software (Access Points for Wireless LAN)

Series	Notes
[illegible]0	RADIUS interoperability
AP1100	RADIUS interoperability
AP1200	Tested with Aironet 11.23 RADIUS interoperability

Table 11 CiscoWorks VMS

Series	Devices Supported	Notes
IOS/Router MC	Version 1.1	TACACS+ interoperability
PIX MC	Version 1.1	Tested with VMS2.1 TACACS+ interoperability
IDS MC	Version 1.1	TACACS+ interoperability
LMS	—	TACACS+ interoperability (future release)
[illegible]SE	Version 1.7	TACACS+ interoperability
WLSE	—	TACACS+ interoperability (future release)

Table 12 PKI/Certificate Servers

Platform	Versions	Notes
Microsoft CA Certificate Server	Windows 2000 Windows 2000 with SP3	Tested

RQS [redacted] 7 - CN
CPMI - CORREIOS
Fls: Nº 363
Doc. 3698

Table 12 PKI/Certificate Servers (continued)

Entrust PKI	Version 6.0	—
Verisign Onsite	Version 5.0	—

Table 13 Token Servers[1]

Platform	Versions	Client Requirement	Notes
ActivCard Server	Version 3.1	—	—
CRYPTOCard CRYPTOAdmin	Version 5.16	—	—
PassGo Defender	Version 4.1.3	—	—
RSA ACE/Server	Version 5.1	—	Tested
Safeword Premier Access	Version 31.	—	—
Vasco Vacman Server	Version 6.0.2	—	—

1. Cisco Secure ACS Appliance uses a RADIUS interface to support all token servers. For more information, see Changes to Token Server Support.

Table 14 LDAP Servers

Platform	Versions	Notes
SunONE Identity Server (Formerly iPlanet Directory)	Version 5.1	Tested with Windows 2000 Active Directory with Windows Service Pack 3
Novell NetWare Directory Services (NDS)	Version 6.0	Tested
Novell eDirectory	Version 8.6	Tested

Table 15 User Databases[1]

Platform	Version	Requirement
SAM on Windows 2000	—	Tested with Service Pack 3

8154
A.

Table 15 User Databases[1] (continued)

AD on Windows 2000	—	—
SAM on Windows NT 4.0	—	—
LDAP	Generic	—
Novell NetWare Directory Services (NDS)	Version 6.0	Tested with eDirectory v.8.6 and Novell Client 4.83 SP2 for Windows NT 4.0, Windows 2000, and Windows XP
LEAP Proxy RADIUS servers	—	—

1. See also Table 13.

Table 16 Proxy Support

Platform	Versions	Notes
Cisco Secure ACS	2.4 or later	—
Funk Steel Belted Radius	Enterprise Edition	—

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 364
Doc. 3698

Doc.
000233

CORREIOS

CORREIOS

CORREIOS

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

HP INVENT – MANUAL APÊNDICES HX A IQ

2003
PASTA 14

ECT
CPMI - CORREIOS
Fls Nº 365
3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 366
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 367
Doc. 3698

VPN Client User Guide for Windows

Release 3.6
August 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: 78-14738-01
Customer Order Number: DOC-7814738=

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 368
3698
Doc.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0206R)

VPN Client User Guide for Windows
Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

CONTENTS

Preface ix

Audience ix

Organization ix

Terminology x

Related documentation x

VPN 3000 Series Concentrator Documentation xi

Conventions xi

Data Formats xii

Obtaining Documentation xiii

World Wide Web xiii

Documentation CD-ROM xiii

Ordering Documentation xiii

Documentation Feedback xiii

Obtaining Technical Assistance xiv

Cisco.com xiv

Technical Assistance Center xiv

Cisco TAC Web Site xv

Cisco TAC Escalation Center xv

CHAPTER 1 **Understanding the Cisco VPN Client** 1-1

How the VPN Client Works 1-2

Connection Technologies 1-2

VPN Client Features 1-3

Program Features 1-3

Windows NT, Windows 2000, and Windows XP Features 1-3

IPSec Features 1-4

Authentication Features 1-4

Firewall Features 1-5

VPN Client IPSec Attributes 1-5

CHAPTER 2 **Installing the VPN Client** 2-1

Installation Applications 2-1

Verifying System Requirements 2-1

Gathering Information You Need 2-2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 369
3698
Doc.

Installing the VPN Client Through InstallShield 2-3
Installing the VPN Client Through Microsoft Windows Installer 2-5
What Next? 2-9

CHAPTER 3 **Configuring the VPN Client** 3-1
How to Get Help 3-1
Determining the VPN Client Version 3-3
What Is a Connection Entry? 3-5
How To Create a New Connection Entry 3-5
Choosing an Authentication Method 3-7
Group Authentication 3-7
Certificate Authentication 3-8
Sending a Certificate Authority Certificate Chain 3-9
Validating a Certificate 3-10
Configuring an Entrust Certificate for Authentication 3-10
Configuring a Connection Entry for a Smart Card 3-11
Smart Cards Supported 3-12
Completing the Connection Wizard 3-13
What Next? 3-13
Setting or Changing Connection Entry Properties 3-14
Changing General Settings 3-17
Changing Connection Entry Description 3-17
Enabling Transparent Tunneling 3-17
Allowing Local LAN Access 3-18
Adjusting the Peer Response Timeout Value 3-19
Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME) 3-20
Changing Authentication Settings 3-20
Changing Group Name or Group Password 3-21
Choosing a Different Certificate 3-22
Changing Connection Settings 3-23
Enabling and Adding Backup Servers 3-23
Removing Backup Servers 3-24
Changing the Order of the Servers 3-24
Disabling Backup Servers 3-24
Configuring a Connection to the Internet Through Dial-up Networking 3-24
Microsoft Dial-up Networking 3-25
Third Party Dial-up Program 3-26
Changing the VPN Device Address for a Connection Entry 3-26

CHAPTER 4 **Connecting to a Private Network** 4-1

Starting the VPN Dialer 4-2

Connection Procedure 4-2

Using the VPN Client to Connect to the Internet via Dial-Up Networking 4-3

Authenticating to Connect to the Private Network 4-4

User Authentication 4-5

Authenticating Through the VPN Device Internal Server or RADIUS Server 4-5

Authenticating Through a Windows NT Domain 4-6

Changing your Password 4-7

Authenticating Through RSA Data Security (RSA) SecurID (SDI) 4-8

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95, Windows 98, and Windows ME) 4-8

RSA User Authentication: SoftID v1.x (Windows NT Only) and SoftID v2.0 (All Operating Systems) 4-9

RSA New PIN Mode 4-9

SecurID Next Cardcode Mode 4-11

Connecting with Digital Certificates 4-11

Connecting with an Entrust Certificate 4-12

Accessing Your Profile 4-12

Entrust Inactivity Timeout 4-14

Using Entrust SignOn and Start Before Logon Together 4-14

Connecting with a Smart Card or Token 4-14

Completing the Private Network Connection 4-16

Using Automatic VPN Initiation 4-16

Connecting Through Auto Initiation 4-17

Disconnecting Your Session 4-19

Changing Option Values While Auto Initiation is Suspended 4-20

Disabling Auto Initiation 4-20

Disabling While Suspended 4-21

Restarting After Disabling Auto Initiation 4-21

Connection Failures 4-22

Summary of Auto Initiation States 4-23

Viewing Connection Status 4-24

General Information 4-24

Statistics 4-26

Secured Routes 4-27

Local LAN Routes 4-27

Time Connected 4-27

Firewall Tab 4-27

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 370
3698
Doc.

AYT Firewall Tab 4-28
Centralized Protection Policy (CPP) Using the Cisco Integrated Client 4-29
Firewall Rules 4-29
Client/Server Firewall Tab 4-31
Resetting Statistics 4-32
Closing the VPN Client 4-32
Disconnecting your VPN Client Connection 4-32

CHAPTER 5 **Managing the VPN Client 5-1**
Managing VPN Client Connection Entries 5-2
Cloning a Connection Entry 5-3
Deleting a Connection Entry 5-4
Renaming a Connection Entry 5-5
Importing a VPN Client Configuration File 5-5
Erasing a Saved Password for a Connection Entry 5-7
Creating a Shortcut for a Connection Entry 5-10
Enabling Stateful Firewall (Always On) 5-11
Launching an Application 5-11
Managing Windows NT Logon Properties 5-14
Starting a Connection Before Logging on to a Windows NT Platform 5-14
What Happens When You Use Start Before Logon 5-15
Turning Off Start Before Logon 5-15
Permission to Launch an Application Before Log On 5-15
Disconnecting When Logging Off of a Windows NT Platform 5-16
Managing Auto Initiation 5-16
Viewing and Managing the VPN Client Event Log 5-17
Starting the Log Viewer 5-18
Displaying the Version of the Software 5-19
Collecting Events 5-19
Filtering Events 5-20
Searching the Log File 5-22
Printing the Log File 5-23
Saving the Log File 5-24
Clearing the Events Display 5-24
Receiving Notifications From a VPN Device 5-25
Upgrade Notifications 5-25
Firewall Notifications 5-26
Upgrading the VPN Client Software (InstallShield) 5-27

Upgrading the VPN Client Software (MSI) 5-29
Uninstalling the VPN Client with the Uninstall Application 5-29
Removing the VPN Client Software MSI Installation 5-32

CHAPTER 6 **Enrolling and Managing Certificates** 6-1
Starting Certificate Manager 6-2
What are Certificate Stores? 6-3
Enrolling for a Certificate 6-4
Enrollment Form 6-4
Starting Enrollment 6-5
Enrolling Through the Network 6-6
Enrolling Through a File Request 6-11
Importing a Certificate File 6-15
Managing Personal and CA/RA Certificates 6-17
Viewing a Certificate 6-18
Verifying a Certificate 6-20
Deleting a Certificate 6-21
Changing the Password on a Personal Certificate 6-22
Exporting a Certificate 6-23
Managing Enrollment Requests 6-25
Viewing the Enrollment Request 6-26
Deleting an Enrollment Request 6-27
Changing the Password on an Enrollment Request 6-28
Completing an Enrollment Request 6-29

APPENDIX A **Copyrights and Licenses** A-1
Client Software License Agreement of Cisco Systems A-1
RSA software A-2
Zone Labs A-3

INDEX

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 371
3698
Doc.

Preface

This *VPN Client User Guide* tells you how to install, use, and manage the Cisco VPN Client with Cisco Systems products.

Audience

This guide is for users of remote clients who want to set up virtual private network (VPN) connections to a central site. Network administrators can also use this guide for information about configuring and managing VPN connections for remote clients. We assume that you are familiar with the Windows platform and know how to use Windows applications. A network administrator should be familiar with Windows system configuration and management and know how to install, configure, and manage internetworking systems. For information specific to a network administrator, see *VPN Client Administrator Guide*.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Understanding the Cisco VPN Client	Explains briefly what the VPN Client is and how it works.
Chapter 2	Installing the VPN Client	Tells you how to install the VPN Client.
Chapter 3	Configuring the VPN Client	Tells you how to configure the VPN Client, including setting optional parameters.
Chapter 4	Connecting to a Private Network	Tells you how to connect to a private network using the VPN Client and an Internet connection; shows how to get status information on your connection, and how to use auto initiation.
Chapter 5	Managing the VPN Client	Tells you how to manage VPN Client connections, upgrade or uninstall VPN Client software, reconfigure the VPN Client automatically, use the Log Viewer application and set up special features such as Start Before Logon.

RQS nº 03/2005 - CN
CPMI - CORREIOS
372
Fls Nº
3698
Doc.

Chapter	Title	Description
Chapter 6	Enrolling and Managing Certificates	Tells you how to obtain digital certificates to use for authentication and how to manage these certificates on your system.
Appendix A	Copyrights and Licenses	Provides copyright and license information for software that the VPN Client uses.

Terminology

In this user guide, the term Cisco VPN device refers to the following Cisco products:

- Cisco VPN 3000 Series Concentrator
- Cisco Secure PIX Firewall devices
- IOS platform devices, such as the Cisco 7100 Series Routers

Related documentation

The VPN Client includes an extensive online HTML-based help system that you can access through a browser in several ways:

- Click the Help icon on the Cisco Systems VPN Client programs menu (Start > Programs > Cisco Systems VPN Client > Help).
- Press **F1** while using the applications.
- Click the **Help** button on screens that include it.

The *VPN Client Administrator Guide* tells a network administrator how to:

- Configure a VPN 3000 Concentrator for several specific features:
  - Configure a VPN 3000 Concentrator for remote access users
  - Configure VPN Client firewall policy on a VPN 3000 Concentrator
  - Notify remote users of a client update
  - Set up Local LAN Access for the VPN Client
  - Configure the VPN Concentrator to update VPN Client backup servers
  - Set up the VPN Concentrator and the VPN Client for NAT Transparency
  - Configure Entrust Entelligence for the VPN Client
  - Set up authentication using Smart Cards.
- Automate remote user profiles
- Configure auto initiation
- Use the VPN Client command-line interface
- Customize the VPN Client software (text, icons and installation)
- Use the SetMTU application
- Obtain troubleshooting information
- Work with Microsoft Windows Installer

The VPN Client guides are provided on the Cisco VPN 3000 Concentrator's software distribution CD-ROM in PDF format. To view the latest version on the Cisco Web site, go to the following site and click **VPN Client**.

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm.

VPN 3000 Series Concentrator Documentation

The *VPN 3000 Concentrator Series Getting Started* guide explains how to unpack and install the VPN Concentrator, and how to configure the minimal parameters. This is known as *Quick Config*.

The *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.

The *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The VPN Concentrator Manager also includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

Other useful books, articles, and websites include:

- *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001
- Kosiur, Dave. *Building and Managing Virtual Private Networks*. Wiley: 1998.
- Sheldon, Tom. *Encyclopedia of Networking*. Osborne/McGraw-Hill: 1998.
- `www.ietf.org` for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).

Conventions

This document uses the following conventions:

Convention	Description
boldface font	User actions and commands are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in `boldface screen` font.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
3698
Doc.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, `192.168.12.34`); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, `255.255.255.0`). Wildcard masks use the same notation (for example, `0.0.0.255`); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, `00.10.5A.1F.4F.07`).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, `VPN01`). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from `0` to `65535`. No commas or spaces are permitted in a number.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

RQS nº 03/2005
CPMI - CORREIOS
Fls. Nº 374
Doc.

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

RQS nº 03/2003 - CPMI - CORREIOS
379
Fls. Nº 3698
Doc.

CHAPTER 1

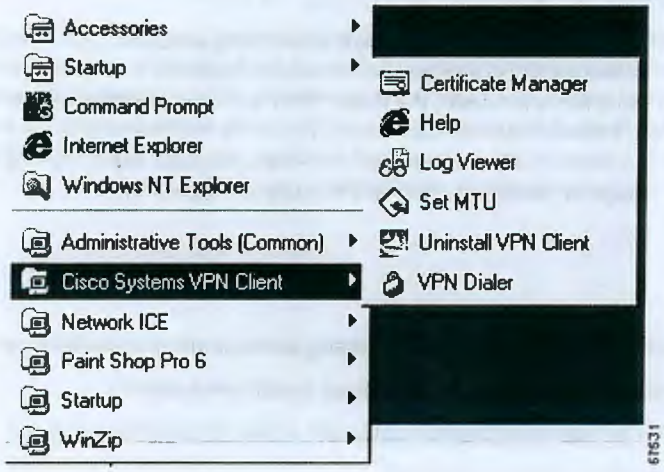
Understanding the Cisco VPN Client

The Cisco VPN Client for Windows (referred to in this user guide as *VPN Client*) is a software program that runs on a Microsoft® Windows®-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN server on an enterprise network or with a service provider, creates a secure connection over the Internet. Through this connection you can access a private network as if you were an on-site user. Thus you have a Virtual Private Network (VPN). The server verifies that incoming connections have up-to-date policies in place before establishing them. Cisco IOS, VPN 3000 Series Concentrators, and PIX central-site servers can all terminate VPN connections from VPN Clients.

As a remote user (low speed or high speed), you first connect to the Internet. Then you use the VPN Client to securely access private enterprise networks through a Cisco VPN server that supports the VPN Client.

The VPN Client comprises the following applications, which you select from the Programs menu:

Figure 1-1 VPN Client Applications as Installed by InstallShield



In logical order of use, the applications are as follows:

- Help—Displays an online manual with instructions on using the applications.
- VPN Dialer—Lets you configure connections to a VPN server and lets you then start your connections.
- Certificate Manager—Lets you enroll for certificates to authenticate your connections to VPN servers.
- Log Viewer—Lets you display events from the log.

RQS nº [redacted] CN
CPMI - CORREIOS
Fls. Nº 376
3698
Doc.

- Uninstall VPN Client—Lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations.

Note There are two ways to install the VPN Client: through the InstallShield wizard or through the Microsoft Installer. If you install the VPN Client through the Microsoft Installer, the Programs menu shown in Figure 1-1 does not contain the Uninstall application.

- SetMTU—Lets you manually change the size of the maximum transmission unit (see the *VPN Client Administrator Guide*, Chapter 6.)

How the VPN Client Works

The VPN Client works with a Cisco VPN server to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:

- Negotiating tunnel parameters—Addresses, algorithms, lifetime, and so on.
- Establishing tunnels according to the parameters.
- Authenticating users—Making sure users are who they say they are, by way of usernames, group names and passwords, and X.509 digital certificates.
- Establishing user access rights—Hours of access, connection time, allowed destinations, allowed protocols, and so on.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

For example, to use a remote PC to read e-mail at your organization, you connect to the Internet, then start the VPN Client and establish a secure connection through the Internet to your organization's private network. When you open your e-mail, the Cisco VPN server uses IPSec to encrypt the e-mail message. It then transmits the message through the tunnel to your VPN Client, which decrypts the message so you can read it on your remote PC. If you reply to the e-mail message, the VPN Client uses IPSec to process and return the message to the private network through the Cisco VPN server.

Connection Technologies

The VPN Client lets you use any of the following technologies to connect to the Internet:

- POTS (Plain Old Telephone Service)—Uses a dial-up modem to connect.
- ISDN (Integrated Services Digital Network)—May use a dial-up modem to connect.
- Cable—Uses a cable modem; always connected.
- DSL (Digital Subscriber Line)—Uses a DSL modem; always connected.

You can also use the VPN Client on a PC with a direct LAN connection.

VPN Client Features

The VPN Client includes the following features:

Program Features

- Complete browser-based context-sensitive HTML-based Help
- Support for VPN 3000 Series Concentrator platforms that run Release 3.0 and above. (VPN Client Release 3.0 and above will not work with Releases 2.x of the VPN 3000 Concentrator.)
- Command-line interface to the VPN Dialer
- Local LAN access—The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission)
- Automatic VPN Client configuration option—the ability to import a configuration file
- Log Viewer—An application that collects events for viewing and analysis
- Set MTU size—The VPN Client automatically sets a size that is optimal for your environment. However, you can set the MTU size manually as well. (For instructions on adjusting the MTU size, see the *VPN Client Administrator Guide).*
- Application Launcher—The ability to launch an application or a third-party dialer from the VPN Client.
- Automatic uninstall of the Nortel Networks VPN Client and the 5000 VPN Client software with the InstallShield installation package
- Automatic connection by way of Microsoft Dial-Up Networking or any other third-party remote access dialer
- Software update notifications from the VPN server upon connection
- Ability to launch a location site containing upgrade software from a VPN server notification
- The ability to automatically initiate secure wireless VPN connections seamlessly
- NAT Transparency (NAT-T), which lets the VPN Client and the VPN Concentrator automatically detect when to use IPSec over UDP to work properly in Port Address Translation environments.
- Update of centrally controlled backup server list—the VPN Client learns the backup VPN Concentrator list through connection establishment. This feature is configured on the VPN 3000 Concentrator and pushed to the VPN Client. The addresses show in the VPN Dialer application in the Enable Backup Servers box under Options->Properties->Connections.
- Support for Dynamic DNS (DDNS hostname population)—The VPN Client sends its hostname to the VPN Concentrator during connection establishment. The VPN Concentrator can send the hostname in a DHCP request that can cause a DNS server to update its database to include the new hostname and Client address.

Windows NT, Windows 2000, and Windows XP Features

- Password expiration information when authenticating through a RADIUS server that references an NT user database. When you log in, the VPN Concentrator sends a message that your password has expired and asks you to enter a new one and then confirm it. On pre-Release 3.5 VPN Clients, the prompt asks you to supply a PIN and to verify it. On a 3.5 or above VPN Client, the prompt asks you to enter and verify a password.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 377
Doc.

- Start Before Logon—The ability to establish a VPN connection before logging on to a Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP systems.
- Ability to disable automatic disconnect when logging off of a Windows NT platform. This allows for roaming profile synchronization.

IPSec Features

- IPSec tunneling protocol
- Transparent tunneling—IPSec over UDP for NAT and PAT, and IPSec over TCP for NAT, PAT, and firewalls
- IKE key management protocol
- IKE Keepalives—Monitoring the continued presence of a peer and reporting the VPN Client's continued presence to the peer. This lets the VPN Client notify you when the peer is no longer present. Another type of keepalives keeps NAT ports alive.
- Split tunneling—The ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel. The VPN Server supplies a list of networks to the VPN Client for tunneled traffic. You enable split tunneling on the VPN Client and configure the network list on the VPN Server, such as the VPN Concentrator.
- Support for Split DNS—The ability to direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN Server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network. For example, a query for a packet destined for *corporate.com* would go through the tunnel to the DNS that serves the private network, while a query for a packet destined for *myfavoritesearch.com* would be handled by the ISP's DNS. This feature is configured on the VPN Server (VPN Concentrator) and enabled on the VPN Client by default. To use Split DNS, you must also have split tunneling configured.
- LZS data compression, which can benefit modem users

Authentication Features

- User authentication by way of VPN central-site device:
  - Internal through the VPN device's database
  - RADIUS (Remote Authentication Dial-In User Service)
  - NT Domain (Windows NT)
  - RSA (formerly SDI) SecurID or SoftID
- Certificate Manager—An application that lets you manage your identity certificates
- Ability to use Entrust Entelligence certificates
- Ability to authenticate using smart cards with certificates
- Peer Certificate Domain Name Verification—prevents a client from connecting to a invalid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.

Firewall Features

- Support for Cisco Secure PIX Firewall platforms that run Release 6.0 and higher

Note Instructions on configuring the VPN Client to interoperate with Cisco Secure PIX Firewall, Release 6.0 and above, are available in *IPSec User Guide for Cisco Secure PIX Firewall.*

- Support for personal firewalls:
  - Cisco Integrated Firewall (CIC)
  - ZoneAlarmPro 2.6.3.57
  - ZoneAlarm 2.6.3.57
  - Zone Integrity
  - BlackIce Agent and BlackIce Defender 2.5
- Centralized Protection Policy—Support for firewall policies pushed to the VPN Client from a VPN Concentrator

VPN Client IPSec Attributes

The VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one of establishing ISAKMP Security Associations (SAs)
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs
- Authentication algorithms:
  - HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function
  - HMAC with SHA-1 (Secure Hash Algorithm) hash function
- Authentication Modes:
  - Preshared Keys
  - X.509 Digital Certificates
- Diffie-Hellman Groups 1(for digital certificates), 2, and 5
- Encryption algorithms:
  - 56-bit DES (Data Encryption Standard)
  - 168-bit Triple-DES
  - AES 128-bit and 256-bit

Note You must be running Release 3.6 of the VPN Client to use the AES encryption algorithm

- Extended Authentication (XAUTH)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 378
3698
Doc.

CHAPTER 2

Installing the VPN Client

This chapter explains how to install the VPN Client on your PC and includes the following sections:

- Verifying System Requirements
- Gathering Information You Need
- Installing the VPN Client Through InstallShield
- Installing the VPN Client Through Microsoft Windows Installer

To upgrade the VPN Client software, or to uninstall it, see "Managing the VPN Client."

Caution Installing the VPN Client software using InstallShield on Windows NT or Windows 2000 requires Administrator privileges. If you do not have Administrator privileges, you must have someone with Administrator privileges install the product for you.

Installation Applications

You can install the VPN Client on your system through two different applications: InstallShield and Microsoft Windows Installer (MSI). Both applications use installation wizards to walk you through the installation. Installing the VPN Client through InstallShield includes an Uninstall icon in the program group; MSI does not. In the latter case, to manually remove VPN Client applications, you can use the Microsoft Add/Remove Programs utility.

Verifying System Requirements

Verify that your computer meets these requirements:

- Computer with a Pentium®-class processor or greater
- One of the following operating systems:
  - Microsoft®Windows® 95 (OSR2), Windows 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT® 4.0 (with Service Pack 6, or higher)
  - Windows 2000
  - Windows XP

RQS nº 03/200
CPMI - CORREIOS
Fls. Nº 379
3698
Doc.

- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 10 MB hard disk space.
- RAM:
  - 16 MB for Windows 95/98
  - 32 MB for Windows NT and Windows ME
  - 64 MB for Windows 2000
  - 128 MB for Windows XP
- To install the VPN Client:
  - CD-ROM drive
  - 3.5 inch high-density diskette drive
  - Administrator privileges if installing on Windows NT or Windows 2000
- To use the VPN Client:
  - Direct network connection (cable or DSL modem and network adapter/interface card)
  - Internal or external modem
  - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, www.microsoft.com. Windows 98 includes the DUN 1.3 functionality.)
- To connect using a digital certificate for authentication:
  - A digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:

    Baltimore Technologies (www.baltimoretechnologies.com)

    Entrust Technologies (www.entrust.com)

    Microsoft Certificate Services—Windows 2000

    Netscape (Security)

    Verisign, Inc. (www.verisign.com)
  - Or a digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

Gathering Information You Need

To configure and use the VPN Client, you may need the information listed in this section.

Ask for this information from the system administrator of the private network you want to access. Your system administrator may have preconfigured much of this data; if so, he or she will tell you which items you need.

- Hostname or IP address of the secure gateway to which you are connecting
- Your IPSec Group Name (for preshared keys)
- Your IPSec Group Password (for preshared keys)
- If authenticating with a digital certificate, the name of the certificate

- If authenticating through the secure gateway's internal server, your username and password
- If authenticating through a RADIUS server, your username and password
- If authenticating through an NT Domain server, your username and password
- If authenticating through a token vendor, your username and PIN
- If authenticating through a smart card, your smart card, reader, PIN or passcode, and the name of the certificate stored on the smart card
- If you should configure backup server connections, the hostnames or IP addresses of the backup servers

Installing the VPN Client Through InstallShield

To install the VPN Client on your system, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.

Step 1 Exit all Windows programs, and disable any antivirus software.

Step 2 Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.

Step 3 Choose **Start > Run**. The Run dialog box appears.

Step 4 Enter E:\VPN Client\CD-ROM\InstallShield\setup.exe, where E: is your system's CD-ROM drive.

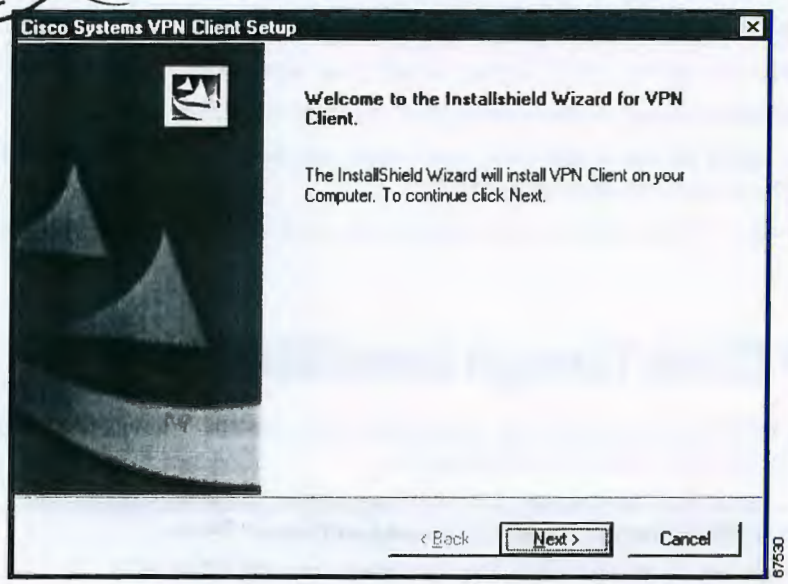
Step 5 Click **OK**.

Note Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

The program displays the Cisco Systems logo and InstallShield Setup window shown in Figure 2-1.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 380
3698
Doc.

Figure 2-1 Starting InstallShield Installation



Step 6 If the InstallShield Wizard identifies an existing version of the VPN Client, the Cisco 5000 Client, or Nortel Networks Extranet Access Client, it displays a dialog box that asks if you want to uninstall the existing client program. To continue, choose **Yes**.

The VPN Client launches the appropriate uninstall wizard: the Cisco VPN Client uninstall wizard to uninstall a previous version of the VPN Client, the Extranet Access Client wizard program, or the Cisco 5000 wizard. Follow the instructions on the uninstall wizard dialog boxes to automatically uninstall the program and reboot.

Note Having more than one VPN client on your system is not advisable.

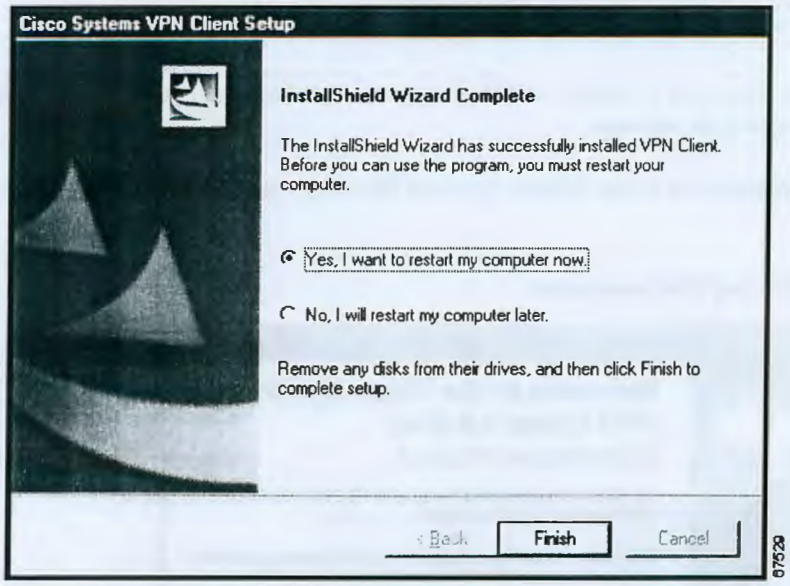
After your system reboots, our own Cisco Systems VPN Client Setup wizard resumes.

Step 7 Follow the instructions on the screens and enter the following information:

A destination folder for the VPN Client files (or click **Next>** to enter the default location C:\Program Files\Cisco Systems\VPN Client).

Step 8 After you have installed the VPN Client, the InstallShield Wizard displays the following screen. You must restart your computer before you can configure and use the VPN Client. (See Figure 2-2.)

Figure 2-2 Completing InstallShield Installation



- To restart now, click **Finish**. Your system reboots. *Be sure to remove any diskette from the drive before you reboot.*
- To restart later, click the **No** radio button and then click **Finish**. The VPN Client Setup closes. Remember: *you must restart your computer before you can use the VPN Client.*

Installing the VPN Client Through Microsoft Windows Installer

Microsoft Windows Installer (MSI) is available for Windows NT, Windows 2000, and Windows XP. To install the VPN Client using MSI, use the following procedure.

Step 1 Exit all Windows programs, and disable any antivirus software.

Step 2 Remove any VPN client software currently on your system including the following applications:

- IRE/SafeNet Client
- Nortel Networks VPN Client
- Altiga VPN Client
- Cisco VPN 3000 Client
- Cisco VPN 5000 Client
- Cisco VPN Client v3.0 through v3.6

To remove these applications, select **Control Panel > Add/Remove Programs**. Select the application and then click **Add/Remove**. After Windows removes the application, you must reboot your system.

Step 3 Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.

Step 4 Choose **Start > Run**. The Run dialog box appears.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 381
3698
Doc.

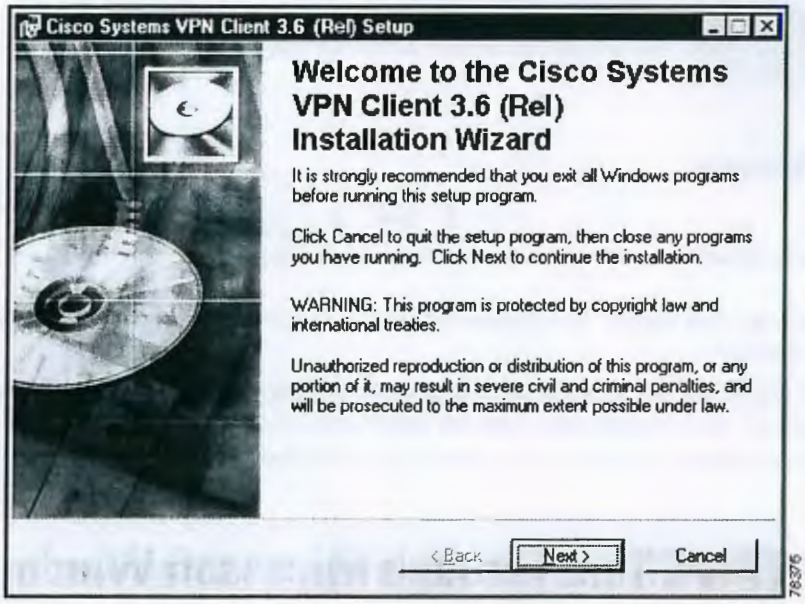
Step 5 Enter E:\VPN Client\CD-ROM\Msi\vpclient_en.exe, where E: is your system's CD-ROM drive.

Step 6 Click **OK**.

Note Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

The program displays the Cisco Systems logo and Microsoft Installer Setup window shown in Figure 2-3.

Figure 2-3 Starting MSI Installation

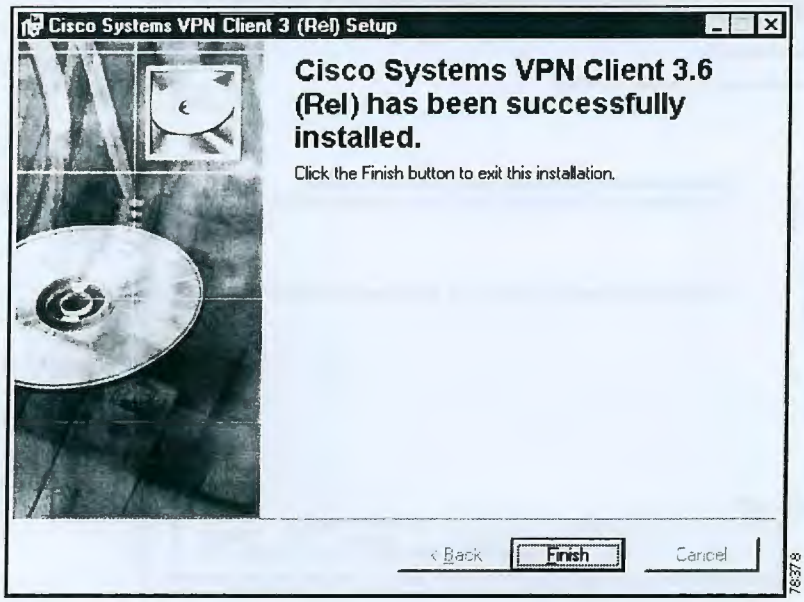


Step 7 Click **Next** to start the installation and then follow the instructions on the dialogs.

MSI installs the VPN Client in the default location C:\Program Files\Cisco Systems\VPN Client. If you want a different destination folder for the VPN Client files, enter the alternative location when prompted to do so.

When the installation has been completed, the installer displays the dialog in Figure 2-4.

Figure 2-4 Completing MSI Installation



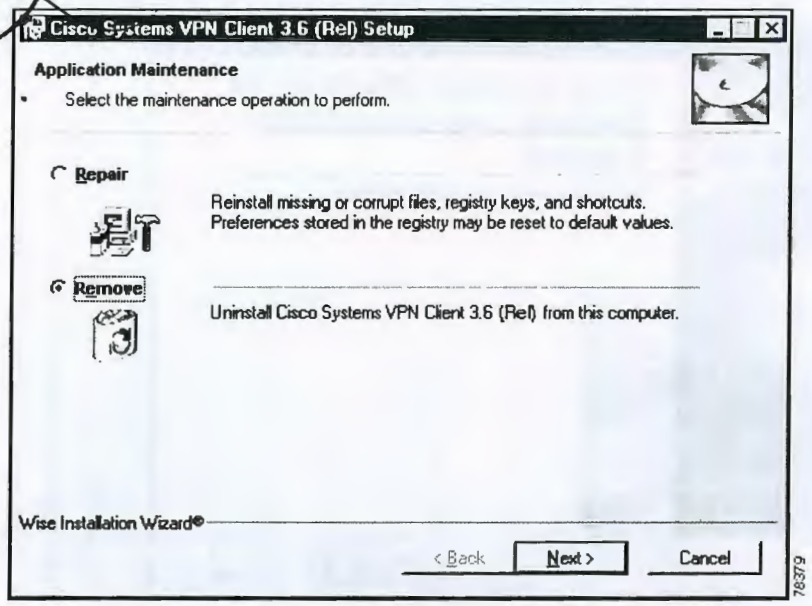
Step 8 Click **Finish**. MSI prompts you to restart your system.

Step 9 Click **Yes** to restart your system.

Note If you have not removed the VPN Client 3.6, when you execute the vpnclient_en.exe command or vpnclien_en.msi, a maintenance and repair wizard displays. See Figure 2-5. You do not see these screens when you remove the software through the Add/Remove programs utility.

RQS nº 03/200
CPMI - CORREIOS
Fls. Nº 382
Doc: 3698

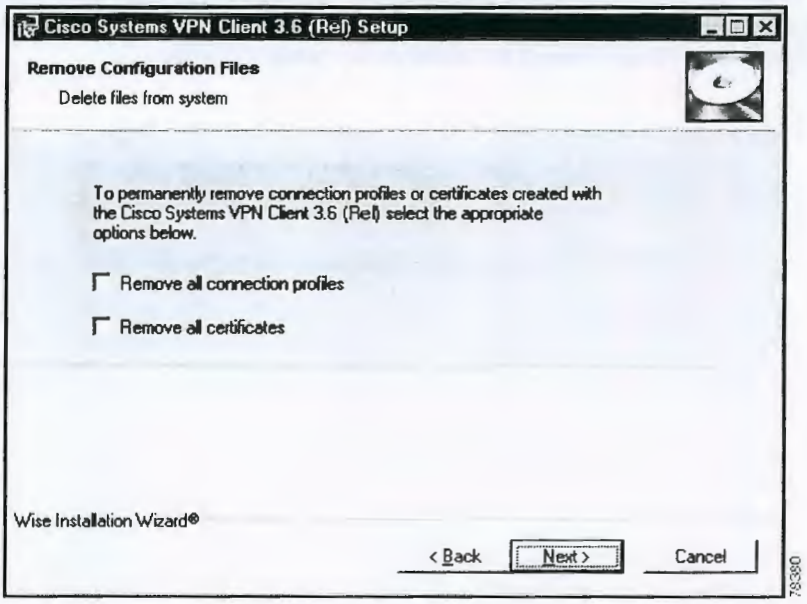
Figure 2-5 Repairing/Removing VPN Client Applications



To remove the VPN Client version 3.6 from your system, follow these steps:

Step 1 Click the **Remove** radio button and then click **Next**. The maintenance wizard displays the Remove Configuration Files dialog. (See Figure 2-6)

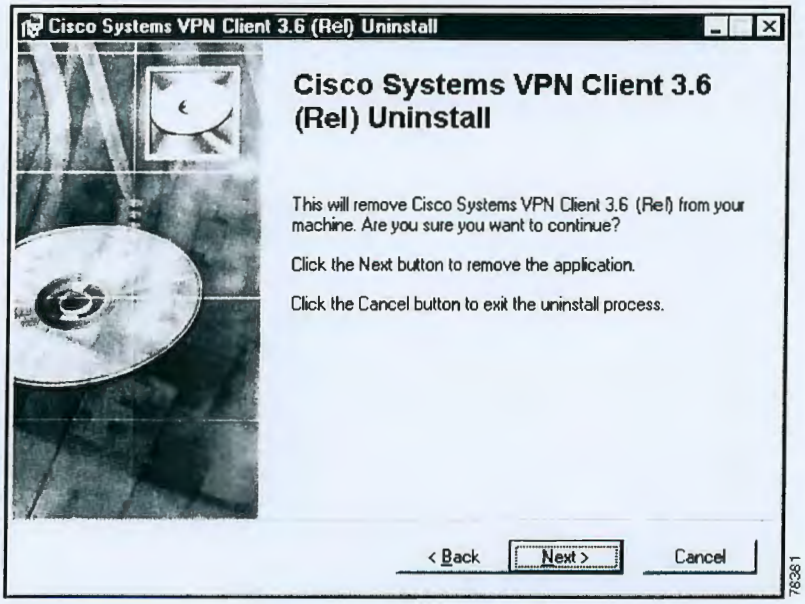
Figure 2-6 Removing Cisco VPN Client 3.6



Step 2 If you want to remove your connection profiles and/or certificates, click the box(es) on the dialog. By default, this wizard does not delete these files. To continue, press **Next**.

The wizard continues and displays the dialog shown in Figure 2-7.

Figure 2-7 Cisco Systems VPN Client 3.6 Uninstall dialog



Step 3 To remove the Cisco VPN Client version 3.6, click **Next**. Or to halt the wizard, click **Cancel**.

When you click Next, the wizard removes the Cisco VPN Client version 3.6. If you elected to remove your connection profiles and/or certificates, these files are also removed; otherwise, these files remain on your system.

When you click Cancel, the wizard prompts you to either Resume or Exit Setup. To stop removal, click **Exit Setup**. If you want to continue the removal, click **Resume**.

What Next?

When the VPN Client software is installed on your PC, to configure it, see "Configuring the VPN Client."

RQS nº 03/2005 - CN
CPMI - CORREIOS
383
Fls. Nº
Doc 3695

CHAPTER 3

Configuring the VPN Client

This chapter explains how to configure the VPN Client.

To configure the VPN Client, you enter values for a set of parameters known as a *connection entry*. The VPN Client uses a connection entry to identify and connect securely to a specific private network.

Parameters include a name and description for the connection, the name or address of the VPN device (remote server), and information that identifies you to the VPN device.

Note If your system administrator has completely configured your connection entry for you, you can skip this chapter and go directly to "Connecting to a Private Network."

This chapter explains the following configuration tasks:

- How to Get Help
- What Is a Connection Entry?
- How To Create a New Connection Entry
- Setting or Changing Connection Entry Properties
- Changing the VPN Device Address for a Connection Entry

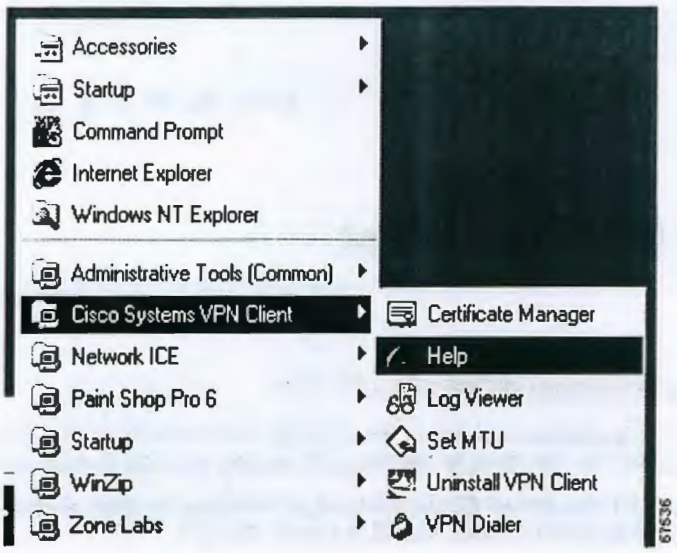
How to Get Help

The VPN Client comes with a complete, context-sensitive, browser-based help system. You can display help in the following ways:

- On the Program Menu, choose **Start > Programs > Cisco Systems VPN Client > Help.** (See Figure 3-1.) This method displays the entire help file beginning with a list of topics.

RQS nº 03/200
CPMI - CORREIOS
Fls. Nº 384
3690
Doc.

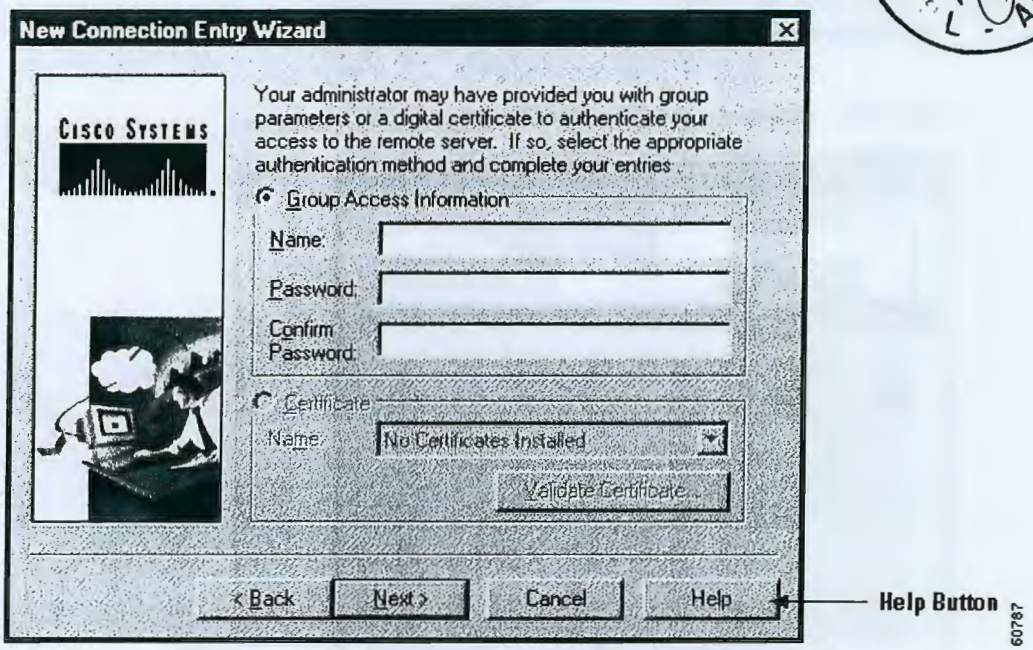
Figure 3-1 Choosing Help from the Cisco Systems VPN Client Program Menu



Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

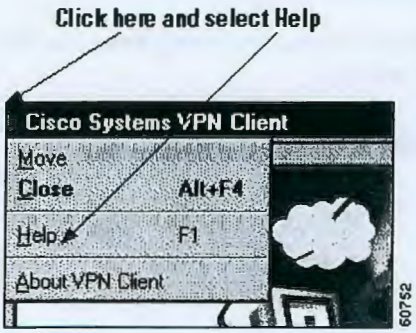
- Press **F1** at any window while using the VPN Client, including the main window of each application (VPN Dialer, Log Viewer, and Certificate Manager). This method displays context-sensitive information.
- Click the **Help** button on windows that display it. (See Figure 3-2.) This method displays context-sensitive information.

Figure 3-2 Help Button



- Choose **Help** from the menu that appears when you click on the icon in the title bar. (See Figure 3-3.)

Figure 3-3 Menu Containing Help Option



Determining the VPN Client Version

To display the version number of the software release you are currently using, follow these steps:

Step 1 Click the icon in the title bar. (See Figure 3-3.)

The VPN Client displays a menu.

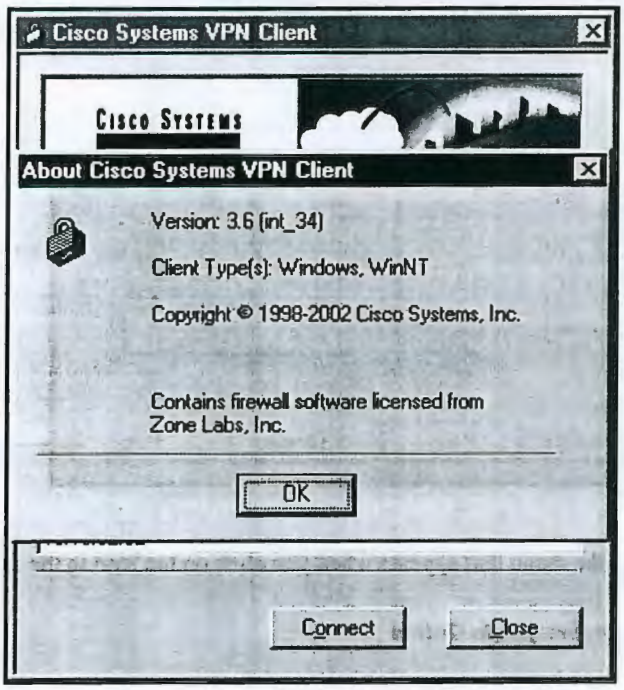
Step 2 Click **About VPN Client** on the menu displayed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 385
3698
Doc.

Step 2 The VPN Client displays the version you are currently using. (See Figure 3-4.)

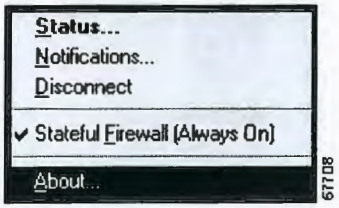
Step 3 After viewing the version number, click **OK**.

Figure 3-4 Displaying the VPN Client Software Version



When you are connected, you can display the software version by clicking **About...** on the menu you display by right clicking the Dialer icon in the system tray.

Figure 3-5 Displaying Version from Menu Available from System Tray



What Is a Connection Entry?

To use the VPN Client, you must create at least one connection entry, which identifies the following information:

- The VPN device (the remote server) to access
- Preshared keys—The IPSec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPSec algorithms your VPN Client uses
- Certificates—The name of the certificate you are using for authentication
- Optional parameters that govern VPN Client operation and connection to the remote network

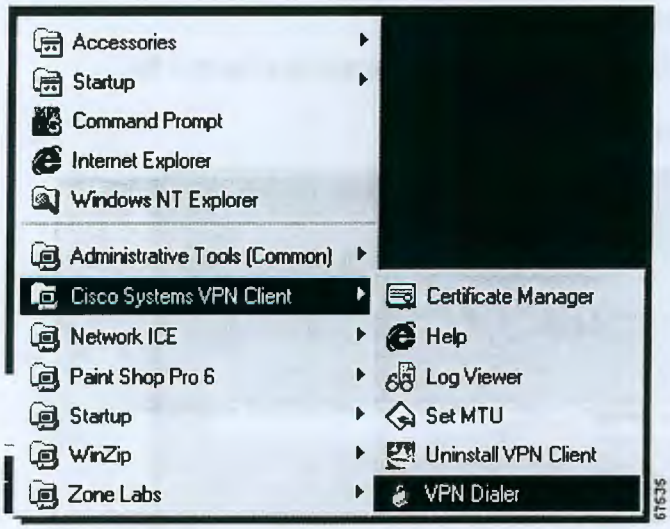
You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously) or if you belong to more than one VPN remote access group.

For connection entry parameters, see "Gathering Information You Need".

How To Create a New Connection Entry

Start the VPN Client by choosing **Start > Programs > Cisco Systems VPN Client > VPN Dialer.**

Figure 3-6 Starting the VPN Dialer

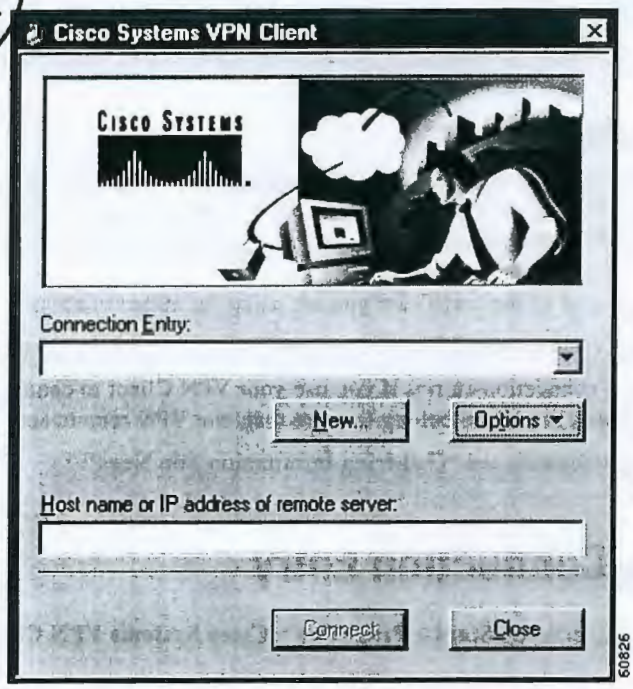


Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

The VPN Dialer application starts and displays its main dialog box. (See Figure 3-7.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 386
3698
Doc.

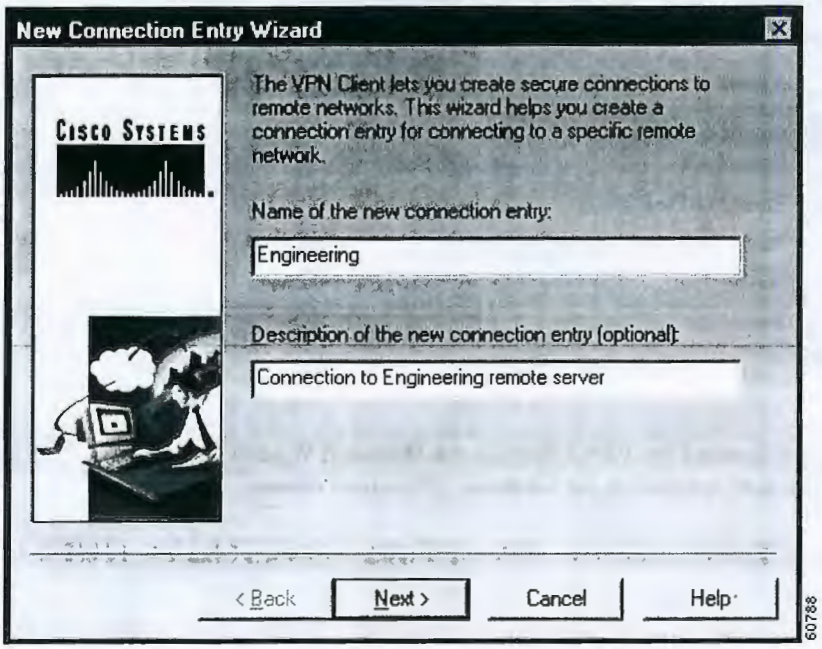
Figure 3-7 VPN Dialer Main Dialog Box



Step 1 At the main dialog, click **New**.

The first New Connection Entry Wizard dialog box appears. (See Figure 3-8.)

Figure 3-8 Entering Name and Description



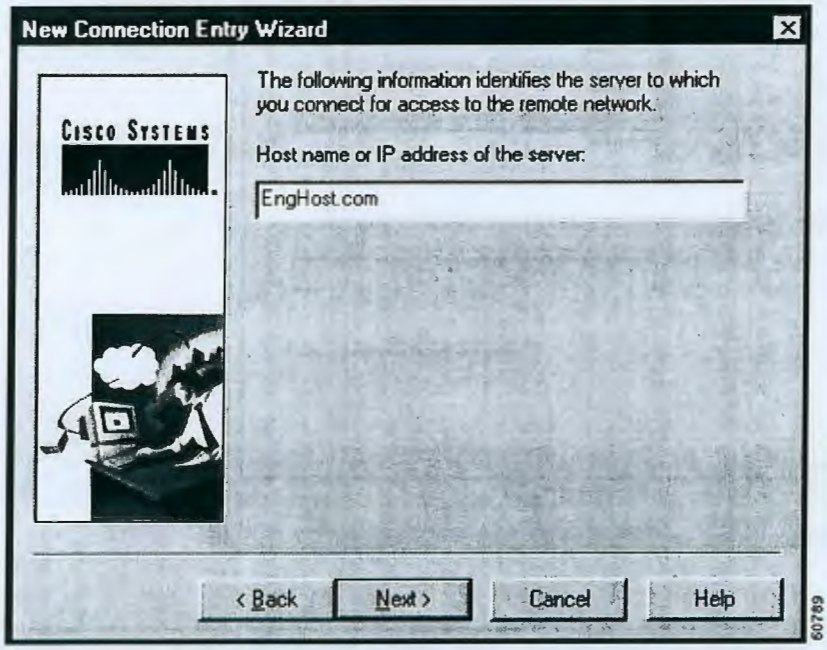
Step 2 Enter a unique name for this new connection. You can use any name to identify this connection, for example, Engineering. This name can contain spaces, and it is not case-sensitive.

Step 3 Enter a description of this connection. This field is optional, but it helps further identify this connection. For example, Connection to Engineering remote server.

Step 4 Click **Next**.

The second New Connection Entry Wizard dialog box appears. (See Figure 3-9.)

Figure 3-9 Identifying Server



Step 5 Enter the hostname or IP address of the remote VPN device you want to access, and click **Next**.

The third New Connection Entry Wizard dialog box appears. (See Figure 3-10.)

Choosing an Authentication Method

You can connect as part of a group (configured on a VPN device) or by supplying an identity digital certificate.

Group Authentication

For group authentication, perform the following procedure: (See Figure 3-10.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 387
Doc. 3698

Figure 3-10 Group Authentication

Step 1 In the Name field, enter the name of the IPSec group to which you belong. This entry is case-sensitive.

Step 2 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

Step 3 Verify your password by entering it again in the Confirm Password field.

Step 4 To continue, click **Next**.

Certificate Authentication

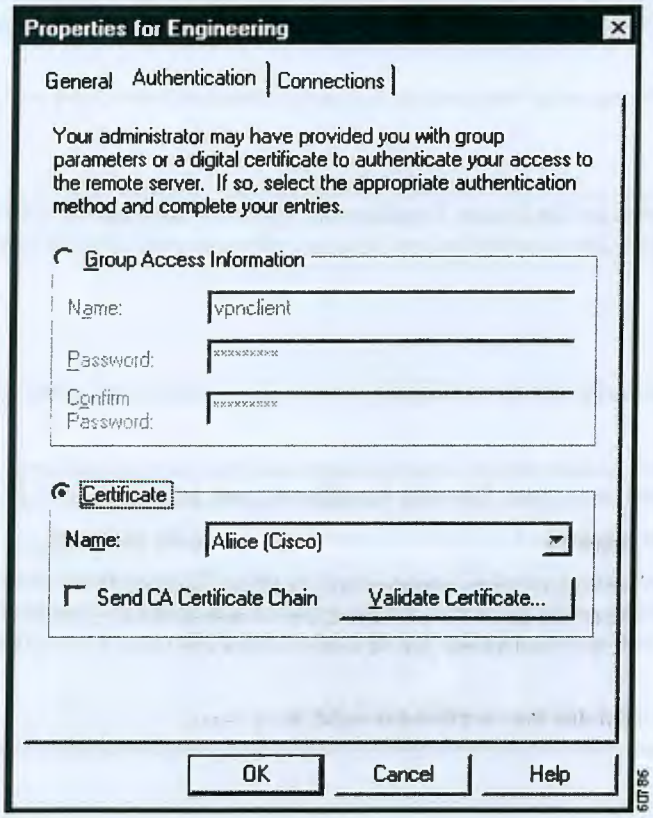
For certificate authentication, perform the following procedure, which varies according the type of certificate you are using:

Step 1 Click the **Certificates** radio button.

Step 2 Choose the name of the certificate you are using from the pull-down menu. (See Figure 3-11.)

If the field says No Certificates Installed and is shaded, then you must first enroll for a certificate before you can use this feature. For information on enrolling for a certificate, see "Enrolling and Managing Certificates" Or, consult your network administrator.

Figure 3-11 Certificate Authentication



Sending a Certificate Authority Certificate Chain

To send CA certificate chains, click **Send CA Certificate Chain**. This parameter is disabled by default.

The CA certificate chain includes all CA certificates in the hierarchy of certificates from the root certificate, which must be installed on the VPN Client, to the identity certificate. This feature enables the a peer VPN Concentrator to trust the VPN Client's identity certificate given the same root certificate, without having all the same subordinate CA certificates actually installed.

Example 3-1 CA Certificate Chains

1. On the VPN Client, you have this chain in the certificate hierarchy:
   - Root Certificate
   - CA Certificate 1
   - CA Certificate 2

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 388
Doc. 3698

- Identity Certificate

2. On the VPN Concentrator, you have this chain in the certificate hierarchy
   - Root Certificate
   - CA Certificate 3
   - Identity Certificate
3. Though the identity certificates are issued by different CA certificates, the VPN Concentrator can still trust the VPN Client's identity certificate, since it has received the chain of certificates installed on the VPN Client PC.

This feature provides flexibility since the intermediate CA certificates don't need to be actually installed on the peer.

Note Certificate chains are not supported for Entrust Entelligence. Therefore the Send CA Certificate Chain checkbox on the Authentication Tab is unchecked and disabled when you select Entelligence Certificate.

Validating a Certificate

Optionally you might want to verify that the certificate you are using is still valid, using the following procedure:

Step 1 To verify the validity of a certificate, click **Validate Certificate...** and enter the password.

If the VPN Dialer prompts for a password to secure the certificate, enter the password.

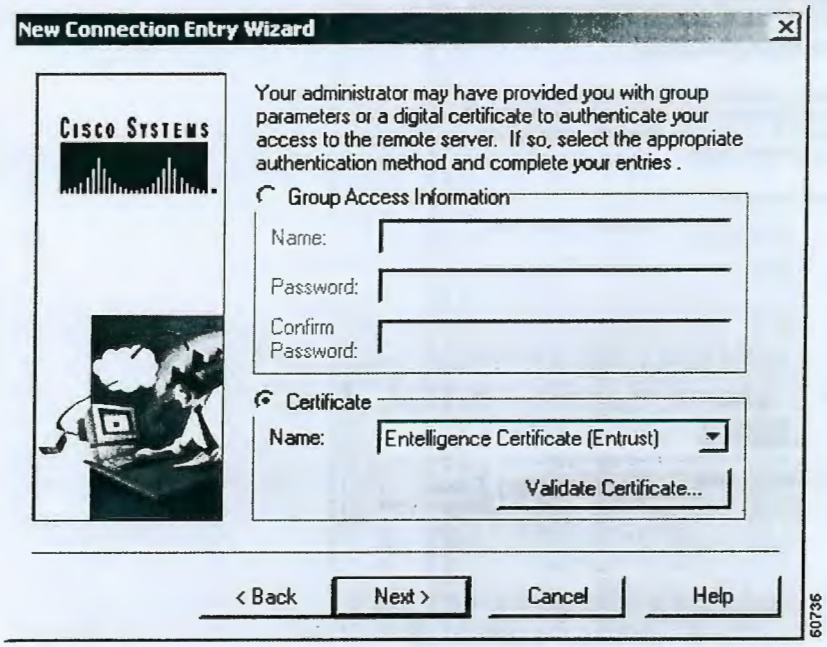
You receive a report letting you know whether the certificate is valid. If the password is not valid, you need to try again. If you do not know the password, see your system administrator. An identity certificate has a public and private key, and a time period within which it is valid. Make sure the certificate is valid before you continue.

Step 2 After you have verified that the certificate is valid, click **Next**.

Configuring an Entrust Certificate for Authentication

If you have an Entrust Entelligence certificate enrolled, the pull-down menu includes the entry "Entelligence Certificate (Entrust)." (See Figure 3-12.)

Figure 3-12 Entrust Entelligence Certificate



An Entrust Entelligence certificate is stored in a *Profile*, which you obtain when you log in to Entrust Entelligence.

Choose **Entelligence Certificate (Entrust)** from the pull-down menu and click **Next**.

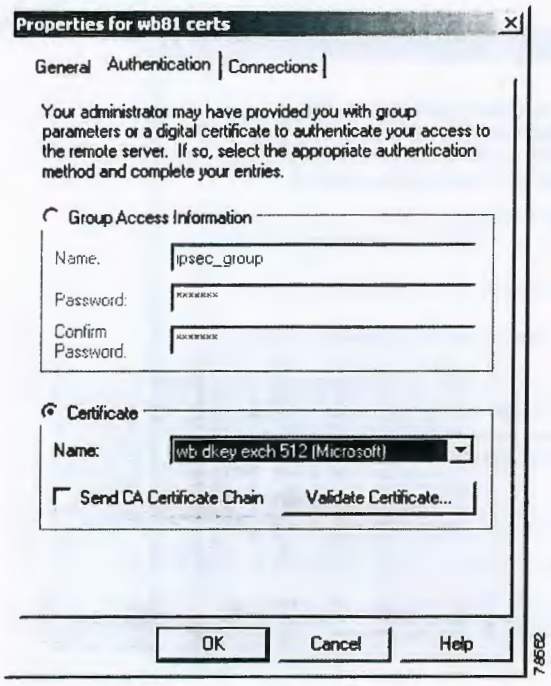
For more information about connecting with Entrust Entelligence, see "Connecting with an Entrust Certificate."

Configuring a Connection Entry for a Smart Card

If you are using a smart card or electronic token to authenticate a connection, create a connection entry that defines the certificate provided by the smart card. For example, if you are using ActivCard Gold, an accompanying certificate is in the Microsoft Certificate Store. When you create a new connection entry for using the smart card, select that certificate. (See Figure 3-13.)

RQS nº 03/2005
CPMI - CORREIOS
Fls. Nº 389
Doc.

Figure 3-13 Creating a Connection Entry for a Smart Card



Smart Cards Supported

The VPN Client supports authentication with digital certificates through a smart card or an electronic token. There are several vendors that provide smart cards and tokens, including the following:

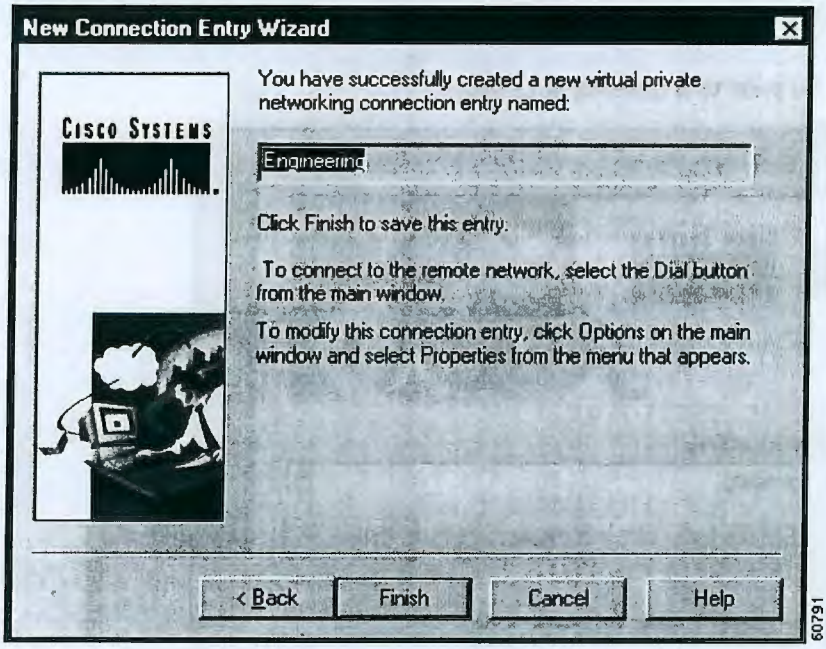
Vendor	Software and Version	Card/Token Tested	Vendor Web site
GemPLUS	GemSAFE Workstation 2.0 or later	GEM195	www.gemplus.com
Activcard	Activcard Gold version 2.0.1 or later	Palmera 32K	www.activcard.com
Aladdin	eToken Runtime Environment (RTE) version 2.6 or later	PRO and R2 tokens	www.ealaddin.com

The VPN Client works only with smart cards and tokens that support CRYPT_NOHASHOID.

Completing the Connection Wizard

After you enter authentication information and click **Next**, the fourth New Connection Entry Wizard dialog box appears. (See Figure 3-14.)

Figure 3-14 Completing the Connection Entry



To complete the connection entry configuration, use the following procedure.

Step 1 Review the connection entry name. If you want to change any previous entries, click **Back** until you get to the desired dialog box.

Step 2 To complete your entry, click **Finish**.

The final New Connection Entry Wizard dialog box closes. Your new connection entry now appears in the Connection Entry drop-down list on the VPN Client's main dialog box.

What Next?

If you need to configure optional connection entry parameters or change parameters for an existing connection entry, continue to the next section.

Otherwise, you can skip to *"Connecting to a Private Network."*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 390
Doc. 3698

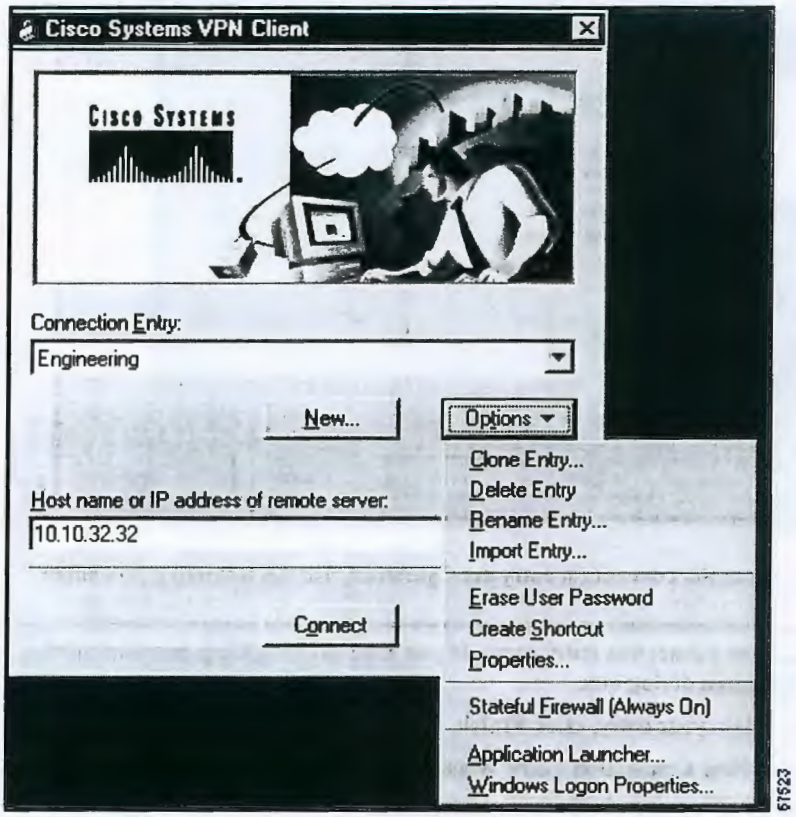
Setting or Changing Connection Entry Properties

To change parameters or to set optional parameters for an existing connection entry, follow these steps:

Step 1 In the VPN Client's main dialog box, click the Connection Entry drop-down menu button and choose the entry you want to configure.

Step 2 Then click **Options** and choose **Properties** from the menu. (See Figure 3-15.)

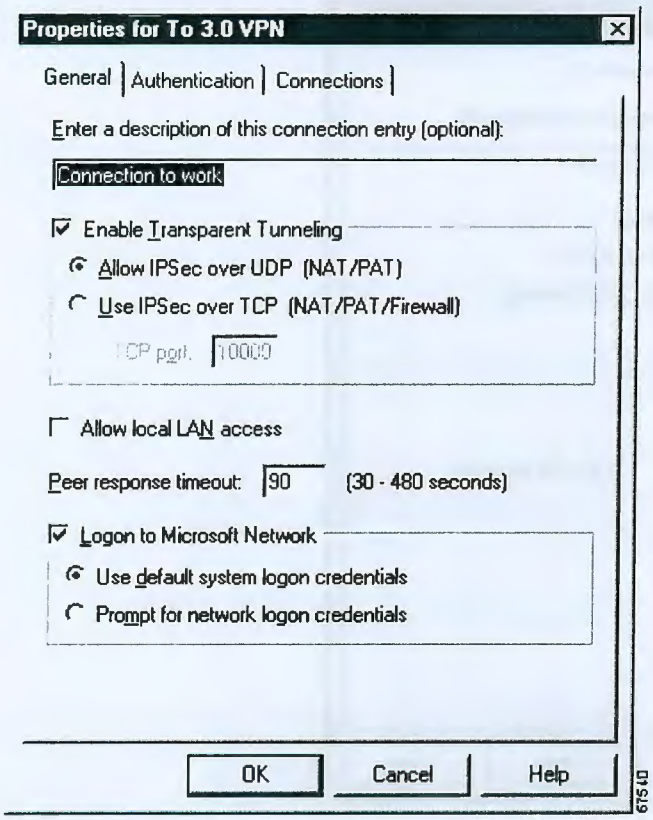
Figure 3-15 VPN Client Options Menu



The Properties dialog box appears. The fields in this dialog box differ according to the operating system you are using.

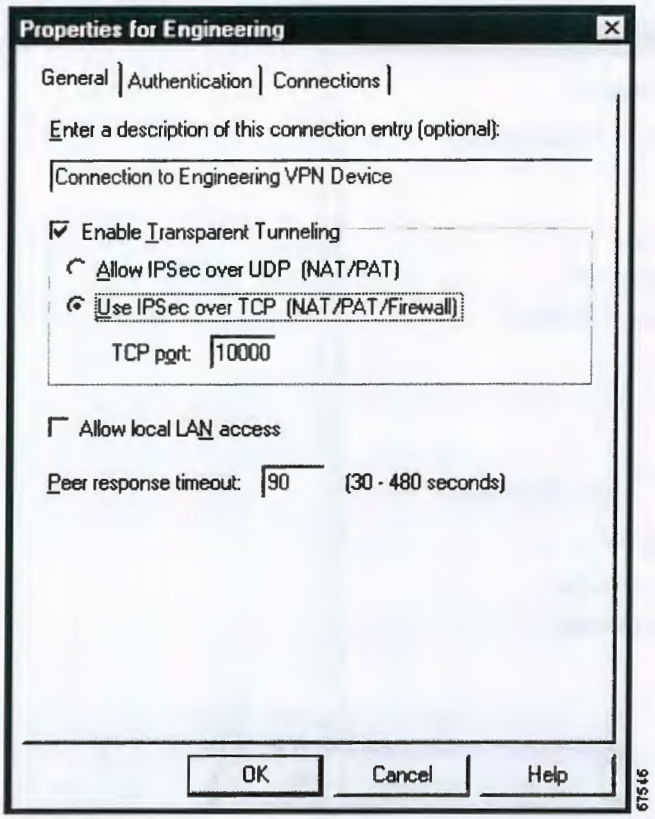
- If you are using Microsoft Windows 95, Windows 98, or Windows ME, you see a dialog box that resembles the one in Figure 3-16.
- If you are using Microsoft Windows NT, Windows 2000, or Windows XP, you see the dialog box in Figure 3-17.

Figure 3-16 Connection Entry Properties Dialog Box (Windows 95, Windows 98 and Windows ME)



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 391
Doc. 3698

Figure 3-17 Connection Entry Properties Dialog Box (Windows NT, Windows 2000, and Windows XP)



Step 3 Click the tab for the parameters you want to change:

- General tab
  - Change the connection entry description
  - Enable transparent tunneling
  - Allow local LAN Access
  - Adjust the peer response time out
  - Log on to Microsoft Network
- Authentication tab
  - Change the group name or group password
  - Change the certificate you want to use
- Connections tab
  - Enable, add, and remove backup server connections
  - Connect to the Internet via Dial-Up Networking

See the appropriate section of this chapter for each tab and parameter.

Step 4 When you have finished setting parameters, click **OK**. The Properties dialog box closes and the VPN Dialer saves your changes.

To discard your changes, click **Cancel**. The Properties dialog box closes and discards all changes.

Changing General Settings

The Properties > General tab lets you set general parameters for this connection entry. (See Figure 3-17.)

Changing Connection Entry Description

To change the description of this connection entry, enter or edit the description field. This field is optional, but it can help you identify this connection.

Enabling Transparent Tunneling

Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT). Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices and/or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.

The VPN Client also sends keepalives frequently, ensuring that the mappings on the devices are kept active.

Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with your device's vendor to verify whether this limitation exists. Some vendors support Protocol-50 (ESP) Port Address Translation (IPSec passthrough), which might let you operate without enabling transparent tunneling.

To use transparent tunneling, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the VPN 3000 Concentrator Manager, Configuration | User Management | Groups | IPSec tab (refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration* or Help in the VPN 3000 Concentrator Manager browser).

This parameter is enabled by default. To disable this parameter, clear the check. We recommend that you always keep this parameter checked.

Then select a mode of transparent tunneling, over UDP or over TCP. The mode you use must match that used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, then in general, TCP mode is preferable. UDP does not operate with stateful firewalls so in this case, you should use TCP.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 392
3698
Doc:

Allow IPSec over UDP (NAT/PAT)

To enable **Allow IPSec over UDP**, click the radio button. With UDP, the port number is negotiated. UDP is the default mode.

Use IPSec over TCP (NAT/PAT/Firewall)

To enable **Use IPSec over TCP**, click the radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

Note When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a client is idle, it does not send a keepalive until it sends data and gets no response.

To allow the VPN Client to work through ESP-aware NAT/Firewalls, add the ForceKeepAlives parameter to the *.pcf (profile configuration file) for the affected connection profile. This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

Use the following syntax when adding this parameter to the [Main] section of any *.pcf file:

ForceKeepAlives=1

For more information, see "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide*.

Allowing Local LAN Access

The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your Client system goes through the IPSec connection to the secure gateway.

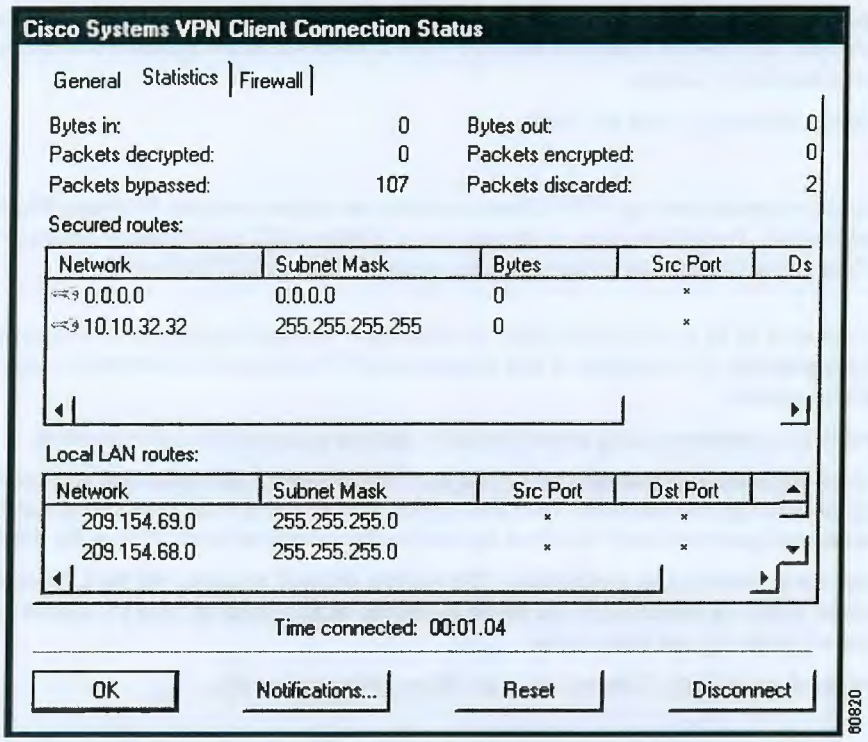
To enable this feature, check **Allow Local LAN Access**; to disable it, clear the check mark from the box. If the local LAN you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the Client side that you can access. You can access up to 10 networks when this feature is enabled. When Allow Local LAN Access is enabled and you are connected to a central site, all traffic from your system goes through the IPSec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking on the Statistics tab on the Connection Status dialog box. (See Figure 3-18.)

Note This feature works only on one NIC card, the same NIC card as the tunnel.

Figure 3-18 Local LAN Access



The Local LAN routes section on the Connection Status dialog box lists the IP address and subnet mask of each available network. The Src Port and Dst Port fields are not currently used.

Note While connected, you cannot print or browse the local LAN by name; when disconnected, you can print and browse by name. For more information on this limitation refer to *VPN Client Administrator Guide,* Chapter 1.

Adjusting the Peer Response Timeout Value

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to check the availability of the VPN device on the other side of an IPSec tunnel. If the network is unusually busy or unreliable, you may need to increase the number of seconds to wait before the VPN Client decides that the peer is no longer active. The default number of seconds to wait before terminating a connection is 90 seconds. The minimum number of seconds you can configure is 30 seconds and the maximum is 480 seconds.

To adjust the setting, enter the number of seconds in the **Peer response timeout** field.

The VPN Client continues to send DPD requests every 5 seconds, until it reaches the number of seconds specified by the Peer response timeout value.

RQS nº 03/2005 - C
CPMI - CORREIOS
Fls. Nº 393
3698
Doc.

Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME)

The **Logon to Microsoft Network** parameter registers your PC on the private Microsoft network and lets you browse and use network resources after the VPN Client establishes a secure connection. This parameter is enabled by default.

To disable this parameter, clear the check.

Note This parameter appears only on VPN Clients installed on systems running Windows 95, Windows 98, and Windows ME. For information on logging on to Windows NT and Windows 2000 systems, see the section "Starting a Connection Before Logging on to a Windows NT Platform."

If you do not need or do not have privileges for Microsoft Windows resources on the private network, disable this parameter. For example, if you require only FTP access to the private network, you could disable this parameter.

If you enable this parameter, click one of the radio buttons to choose the logon process:

Use default system logon credentials—Use the Windows logon username and password on your PC to log on to the private network. With this option, you do not need to manually enter your logon username and password each time you connect to the private network. This is the default selection.

Prompt for network logon credentials—The private network prompts you for a username and password to use its resources. If the logon username or password on your PC differs from those on the private network, use this option.

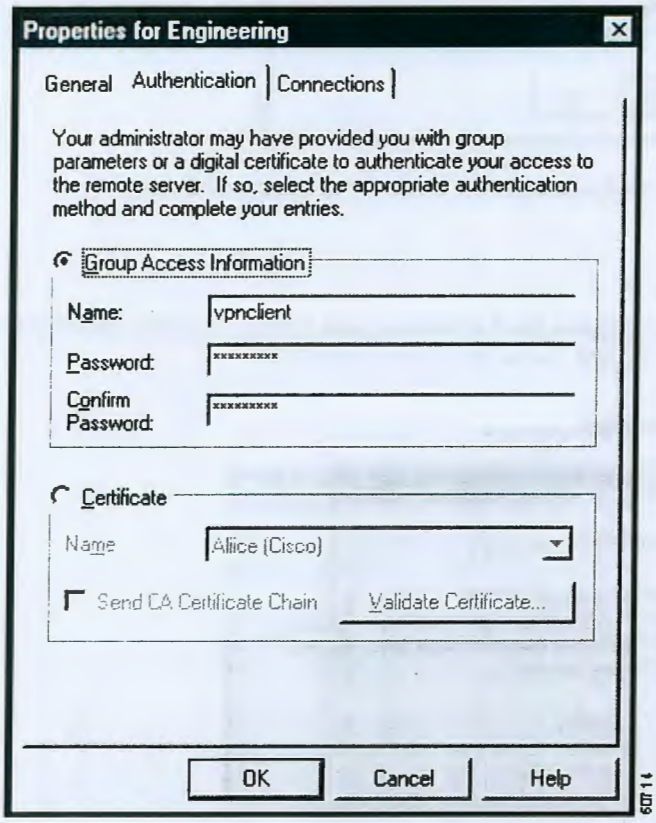
When you are done with the General tab, click **OK** or click another tab.

Changing Authentication Settings

The Properties > Authentication tab (see Figure 3-19) lets you change the name or password of the IPSec group to which you are assigned. Your group determines your access to, and use of, the remote network. The group name and password are essential parameters in authenticating you as a user of the remote network.

If you want to choose a different certificate, you also use this screen.

Figure 3-19 Changing Authentication Parameters from the Authentication Tab



Changing Group Name or Group Password

You usually specify a group name and group password when you create a connection entry. However, you can use the Authentication tab to change a group name or group password if your system administrator so instructs you; or to enter the group name and password if the connection entry does not already have them.

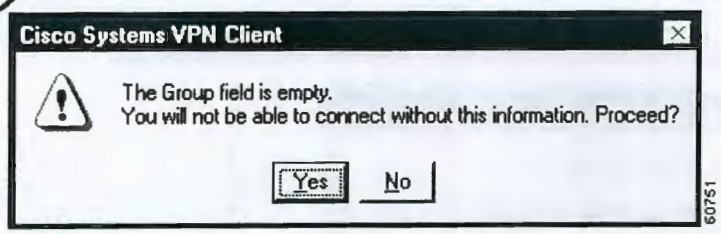
In the Name field, enter or edit the group name. This entry is case-sensitive.

In the Password field, enter or edit the group password. This entry is case-sensitive. The field displays only asterisks. Verify your password by entering it again in the Confirm Password field.

If either field is empty when you leave this dialog box, the VPN Client reminds you to enter missing group information. (See Figure 3-20.) To proceed, click **Yes**, or to terminate, click **No**. If you click No, the message closes, which lets you enter the missing information.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 394
3698
Doc.

Figure 3-20 Reminder Dialog Box

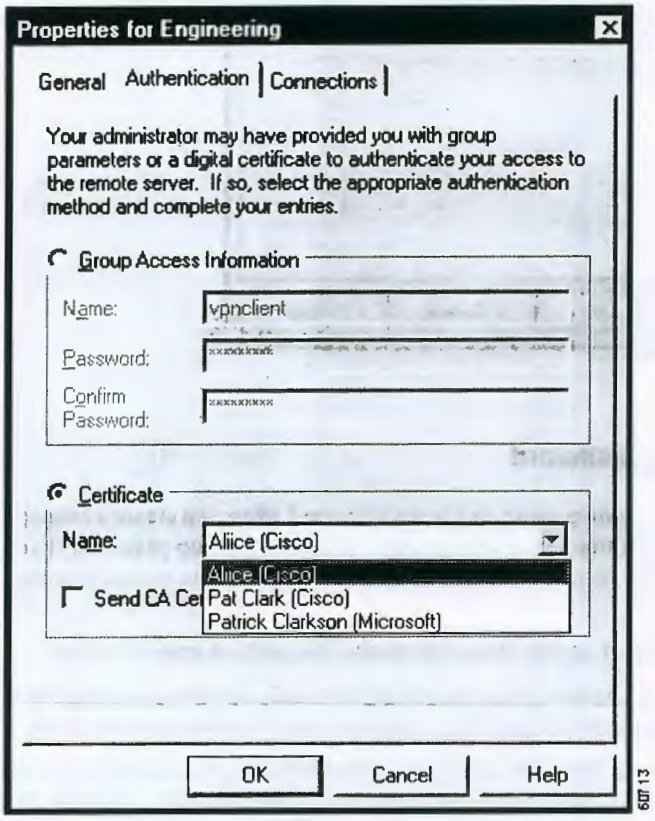


When you are done with the Authentication tab, click **OK** or click another tab.

Choosing a Different Certificate

To choose a different certificate, check the **Certificate** radio button, then click the drop-down menu of certificates installed on your PC and choose one. (See Figure 3-21.)

Figure 3-21 Choosing a Certificate

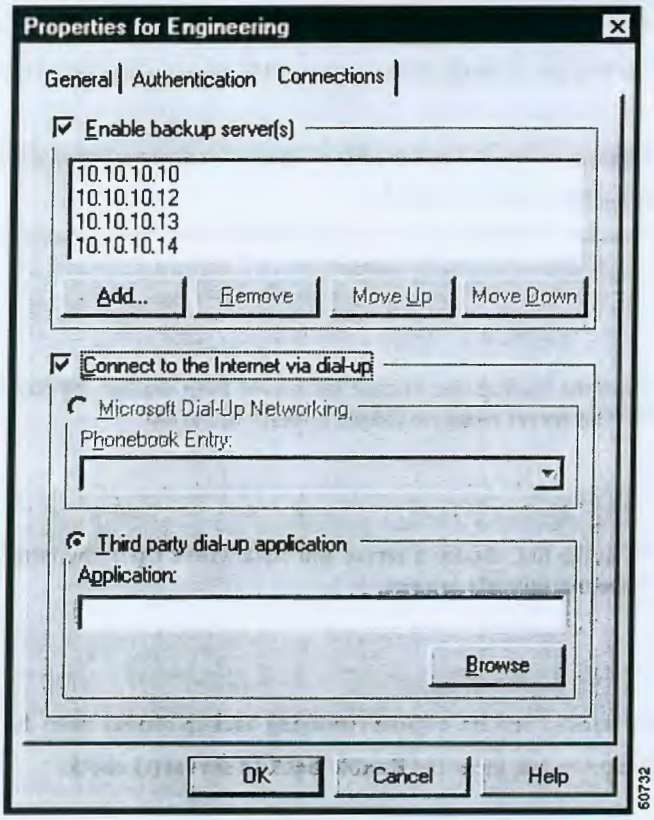


When you are done with the Authentication tab, click **OK** or click another tab.

Changing Connection Settings

The Properties > Connections tab (shown in Figure 3-22) lets you set parameters that govern how you connect to the private network. You can enable and configure backup server connections, and automatically launch a dial-up networking application to connect to the Internet.

Figure 3-22 Changing Parameter Values from the Connections tab



Enabling and Adding Backup Servers

The private network may include one or more backup VPN servers to use if the primary server is not available.Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the VPN Concentrator or you can manually enter this information.

To enable backup servers from the VPN Client, perform the following steps:

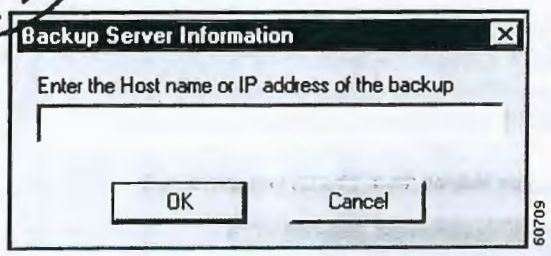
Step 1 Check **Enable backup server(s)**. This is not checked by default.

Step 2 Click **Add** to enter its address.

The Backup Server Information dialog box appears. (See Figure 3-23.)

RQS nº 03/20
CPMI - CORREIOS
Fls. Nº 395
3698
Doc.

Figure 3-23 Entering Backup Server Information



Step 3 Enter the hostname or IP address of the backup server. Use a maximum of 255 characters.

Step 4 Click **OK**.

The hostname or IP address appears in the Enable backup server(s) list. (See Figure 3-22.)

Step 5 To add more backup devices, repeat Steps 2, 3, and 4.

Removing Backup Servers

To remove a server from the backup list, choose the server from the list and click **Remove**. *There is no confirmation or undo.* The server name no longer appears in the list.

Changing the Order of the Servers

To reorder the servers in the list, choose a server and click **Move Up** to increase the server's priority or **Move Down** to decrease the server's priority.

Disabling Backup Servers

You can disable using backup servers without removing backup servers from the list.

To disable using backup servers, clear the **Enable backup server(s)** check.

Configuring a Connection to the Internet Through Dial-up Networking

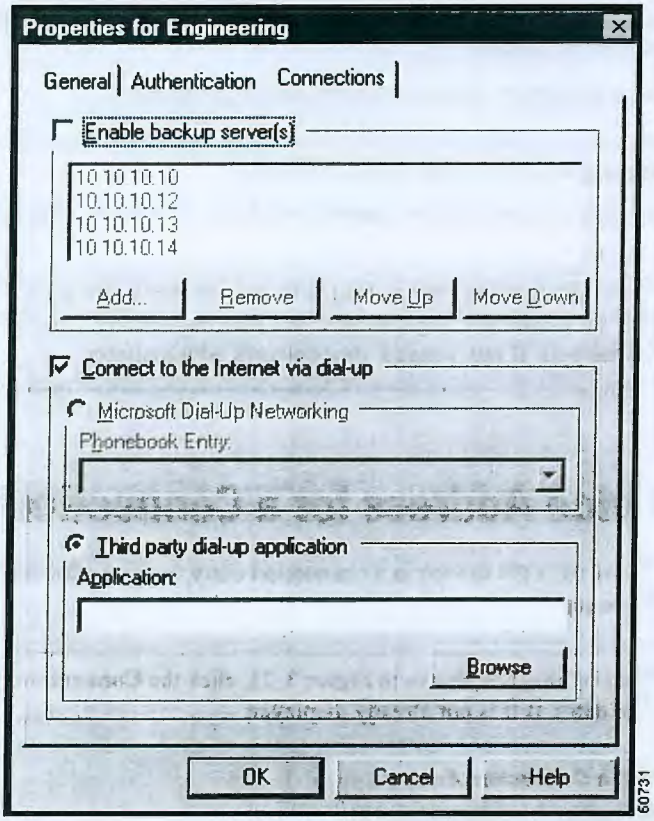
To connect to a private network using a dial-up connection, perform the following two steps:

Step 1 Use a dial-up connection to your Internet service provider (ISP) to connect to the Internet.

Step 2 Use the VPN Client to connect to the private network through the Internet.

To enable and configure this feature, check **Connect to the Internet via dial-up**. This is not checked by default. (See Figure 3-24.)

Figure 3-24 Connecting to the Internet Through Dial-up



You can connect to the Internet using the VPN Dialer application in two different ways:

- Microsoft Dial-up Networking (DUN)
- Third party dial-up program

Microsoft Dial-up Networking

If you have DUN phonebook entries and have enabled Connect to the Internet via dial-up, Microsoft Dial-up Networking is enabled by default. To link a VPN Client connection entry to a Dial-Up Networking phonebook entry, perform the following steps:

Step 1 Click **Microsoft Dial-up Networking** (if it is not already enabled).

Step 2 To link your VPN Client connection entry to a DUN entry, click the down arrow next to the Phonebook entry field and choose an entry from the drop-down menu.

The VPN Client then uses this DUN entry to automatically dial into the Microsoft network before making the VPN connection to the private network.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 396
3698
Doc.

Third Party Dial-up Program

If you have no DUN phonebook entries and have enabled Connect to the Internet via dial-up, then Third party dial-up application is enabled by default.

To connect to the Internet using a third party dial-up program, follow these steps:

Step 1 Click **Third party dial-up application**, if it is not already enabled.

Step 2 Use **Browse** to enter the name of the program in the **Application** field. This application launches the connection to the Internet.

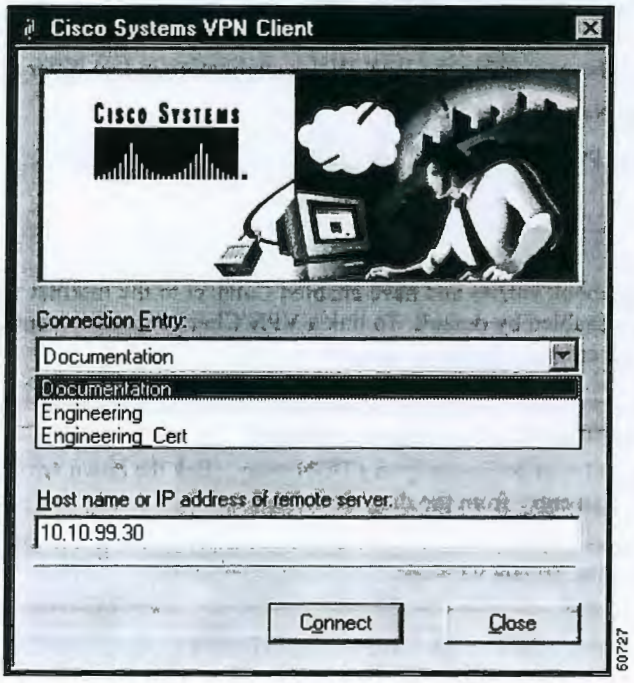
This string you choose or enter here is the pathname to the command that starts the application and the name of the command; for example: c:\isp\ispdialer.exe dialEngineering. Your network administrator might have set this up for you. If not, consult your network administrator.

Changing the VPN Device Address for a Connection Entry

To change the address of the VPN device in a connection entry, and to make the change temporary or permanent, follow these steps:

Step 1 On the VPN Client main dialog box shown in Figure 3-25, click the **Connection Entry** drop-down menu button and choose the entry, if it is not already displayed.

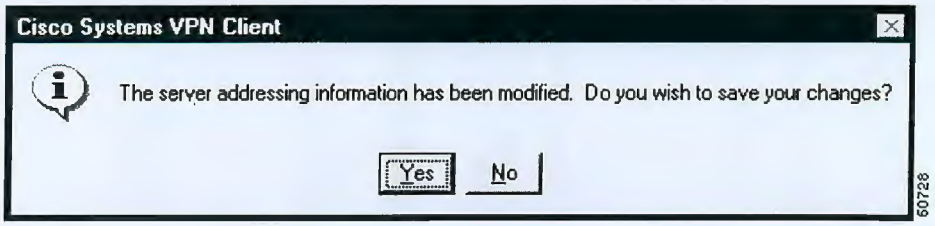
Figure 3-25 Choosing a Connection Entry



Step 2 Edit the address in the Host name or IP address of remote server field.

Step 3 Click **Connect**. The VPN Client displays a confirmation dialog box. (See Figure 3-26.)

Figure 3-26 Confirming Your Changes



Step 4 Click one of the following:

To use this address for the current session only, click **No**. The VPN Client begins connecting to the VPN device, but it does not save the change you have made to the connection entry.

To permanently change the address for this connection entry, click **Yes**. The VPN Client begins connecting to the VPN device, and it saves the new address with the connection entry.

For an explanation of the connection process, see "Connection Procedure".

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 397
3698
Doc.

CHAPTER 4

Connecting to a Private Network

This chapter explains how to connect to a private network with the VPN Client.

We assume you have configured at least one VPN Client connection entry as described in "Configuring the VPN Client." To connect to a private network, you also need the following information:

- ISP logon username and password, if necessary.
- User authentication information:
  - If you are authenticated via the VPN 3000 Concentrator internal server, your username and password.
  - If you are authenticated via a RADIUS server, your username and password.
  - If you are authenticated via an Windows NT Domain server, your username, password, and domain name.
  - If you are authenticated via RSA Data Security (formerly SDI) SecurID or SoftID, your username and PIN.
  - If you use a digital certificate for authentication, the name of the certificate and your username and password. If your private key is password protected for security reasons, you also need this password.

Refer to your entries in "Gathering Information You Need," as you complete the steps described here, which include the following sections:

- Starting the VPN Dialer
- Using the VPN Client to Connect to the Internet via Dial-Up Networking
- Authenticating to Connect to the Private Network
- Connecting with Digital Certificates
- Viewing Connection Status
- Closing the VPN Client
- Disconnecting your VPN Client Connection

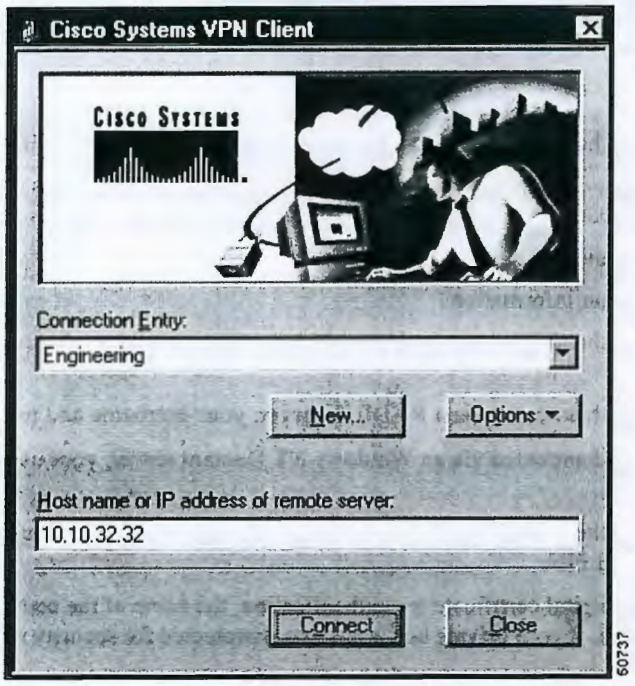
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 398
3698
Doc.

Starting the VPN Dialer

Step 1 To start the VPN Dialer application, choose **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

The VPN Dialer displays the VPN Client's main dialog box. (See Figure 4-1.)

Figure 4-1 VPN Dialer Main Dialog Box



Step 2 If necessary, click the **Connection Entry** drop-down menu and choose the desired connection entry.

Connection Procedure

To connect to a private network, perform the following steps:

Step 1 Connect to the Internet, if necessary.

Step 2 Connect to the private network through the Internet.

- Systems with cable or DSL modems are usually connected to the Internet, so no additional action is necessary. Skip to "Authenticating to Connect to the Private Network."
- Systems with modems or ISDN modems must connect to the Internet via Dial-Up Networking:
  - If you connect to the Internet via Dial-up Networking, proceed to "Using the VPN Client to Connect to the Internet via Dial-Up Networking."

- If you must manually connect to the Internet, do it now. When your connection is established, skip to "Authenticating to Connect to the Private Network."
- If your system is already connected to the Internet via Dial-Up Networking, skip to "Authenticating to Connect to the Private Network."

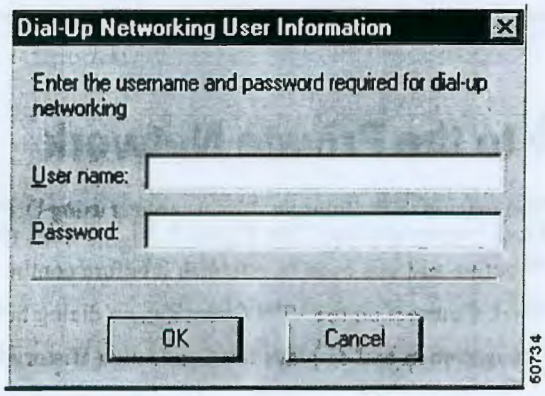
Using the VPN Client to Connect to the Internet via Dial-Up Networking

This section describes how to connect to the Internet via Dial-Up Networking by running only the VPN Client. Your connection entry must be configured with Connect to the Internet via Dial-Up Networking enabled; see "Configuring the VPN Client".

Step 1 Click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

If your credentials are not stored in the RAS database, the Dial-up Networking User Information dialog box appears. (See Figure 4-2.) This dialog box varies depending on the version of Windows you are using.

Figure 4-2 Entering User Information



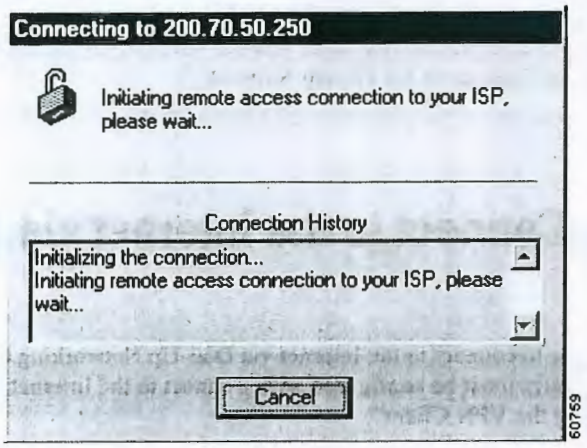
Step 2 Enter your username and password to access your ISP. These entries may be case-sensitive. The Password field displays only asterisks.

Step 3 Click **OK**.

You see the Connection History dialog box. (See Figure 4-3.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 399
3698
Doc.

Figure 4-3 Confirming Connections to ISP



When the ISP connection is established, a Dial-Up Networking icon appears in the system tray on the Windows task bar. (See Figure 4-4.)

Figure 4-4 Dial-Up Networking task bar Icon

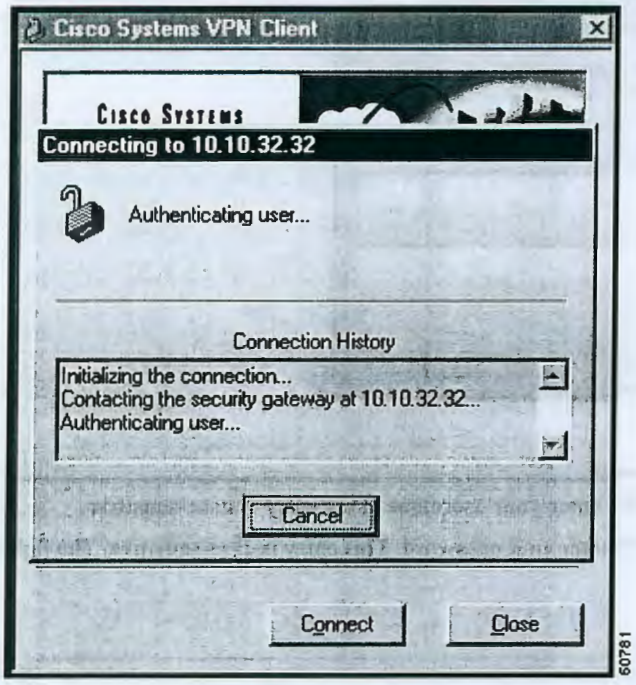
Authenticating to Connect to the Private Network

This section assumes you are connected to the Internet. If you connect using Dial-Up Networking, verify that its icon is visible in the Windows task bar system tray. (See Figure 4-4.) If not, your Dial-Up Networking connection is not active and you need to establish it before continuing.

If you did not do so earlier, click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

The VPN Client starts tunnel negotiation and displays the Connection History dialog box. (See Figure 4-5.)

Figure 4-5 Negotiating Dialog Box



The next phase in tunnel negotiation is user authentication.

User Authentication

User authentication means proving that you are a valid user of this private network. User authentication is optional. Your administrator determines whether it is required.

The VPN Client displays a user authentication dialog box that differs according to the authentication that your IPSec group uses. Your system administrator tells you which method to use.

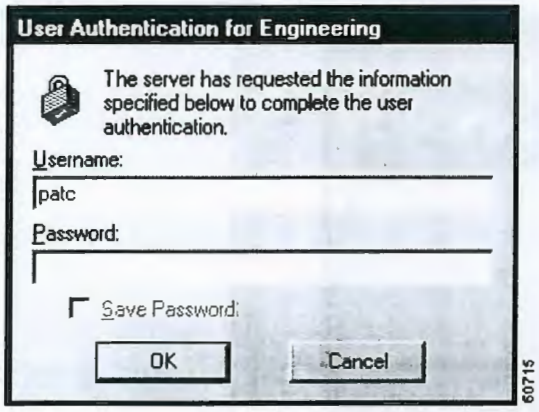
To continue, refer to your entries in "Gathering Information You Need" and go to the appropriate authentication section that follows.

Authenticating Through the VPN Device Internal Server or RADIUS Server

To display the user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 100
3698
Doc.

Figure 4-6 Authenticating Through an Internal or RADIUS Server



Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 Click **OK**.

Note If you cannot choose the Save Password option, your administrator does not allow this option. If you can choose this option, be aware that using it might compromise system security, since your password is then stored on your PC and is available to anyone who uses your PC.

If Save Password is checked and authentication fails, your password may be invalid. To eliminate a saved password, click **Options** > **Erase User Password**.

Proceed to the section "Viewing Connection Status."

Authenticating Through a Windows NT Domain

To display the Windows NT Domain user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

Figure 4-7 Authenticating Through a Windows NT Domain

Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 In the Domain field, enter your Windows NT Domain name, if it is not already there.

Step 4 Click **OK**.

Skip to "Viewing Connection Status."

Changing your Password

Your network administrator may have configured your group for RADIUS with Expiry authentication on the VPN 3000 Concentrator. If this feature is in effect and your password has expired, a dialog box prompts you to enter and confirm a new password.

After you have tried unsuccessfully to log in three times, you might receive one of the following login messages:

- Restricted login hours
- Account disabled
- No dial-in permission
- Error changing password
- Authentication failure

These messages let you know the cause of your inability to log in. For help, contact your network administrator.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 401
3698
Doc.

Authenticating Through RSA Data Security (RSA) SecurID (SDI)

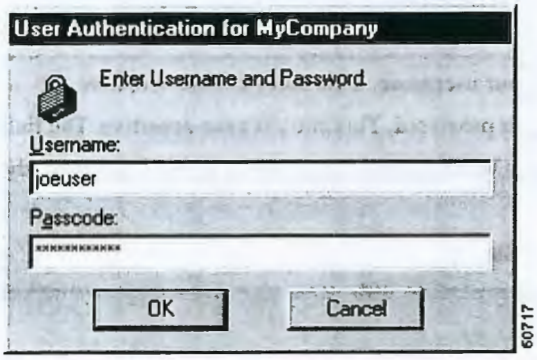
RSA (formerly SDI) SecurID authentication methods include physical SecurID cards and keychain fobs, and PC software called SoftID. SecurID cards also vary: with some cards, the passcode is a combination of a PIN and a cardcode; with others, you enter a PIN on the card and it displays a passcode. Ask your system administrator for the correct procedure.

Authentication via these methods also varies slightly for different operating systems. If you use an RSA method, the VPN Client displays the appropriate RSA user authentication dialog box. The title bar identifies the connection entry name.

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95, Windows 98, and Windows ME)

To display an authentication dialog box asking for your username and passcode, perform the following steps. (See Figure 4-8.) If you are using SoftID, it must be running on your PC.

Figure 4-8 Authenticating through RSA



Step 1 In the Username field, enter your username. This entry is case-sensitive.

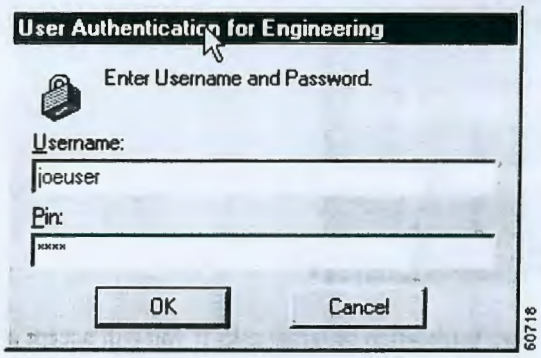
Step 2 In the Passcode field, enter a SecurID code. With SoftID, you can copy this code from the SoftID window and paste it here. Your administrator will tell you what you need to enter here, depending on the type of tokencard you are using.

Step 3 After entering the code, click **OK**.

RSA User Authentication: SoftID v1.x (Windows NT Only) and SoftID v2.0 (All Operating Systems)

If you are using SoftID under Windows NT, the VPN Client displays an authentication dialog box asking for your username and PIN. (See Figure 4-9).

Figure 4-9 Authenticating Through SoftID on Windows NT



Step 1 In the Username field, enter your username. This entry is case-sensitive.

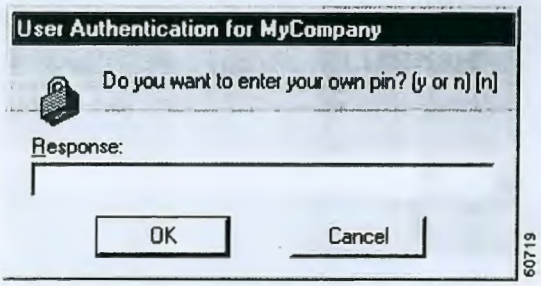
Step 2 In the PIN field, enter your SoftID PIN. The VPN Client gets the passcode from SoftID by communicating directly with SoftID. The SoftID application must be installed but does not have to be running on your PC.

Step 3 After entering the PIN, click **OK**.

RSA New PIN Mode

The first time you authenticate using SecurID or SoftID (all operating systems), or if you are using a new SecurID card, and if the RSA administrator allows you to create your own PIN, the authentication program asks if you want to create your own PIN. (See Figure 4-10.)

Figure 4-10 SecurID New PIN Request

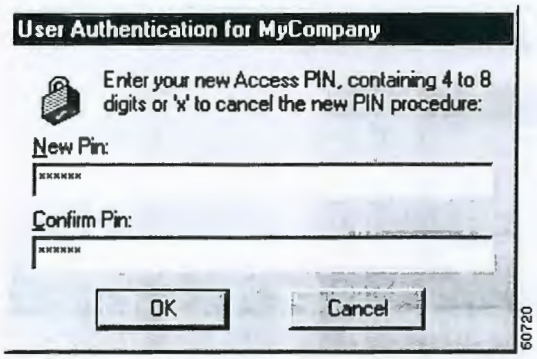


Step 1 Enter your response y for yes or n for no. No is the default response. Then, click **OK**. What happens next depends on your response.

RQS nº 03/200
CPMI - CORREIOS
Fls. Nº 462
3698
Doc.

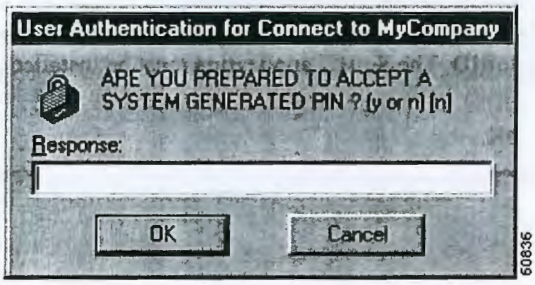
- If you responded yes—Enter your new PIN in the New PIN field and enter it again in the Confirm PIN field. Click **OK**. (See Figure 4-11.)

Figure 4-11 Entering a New PIN Yourself



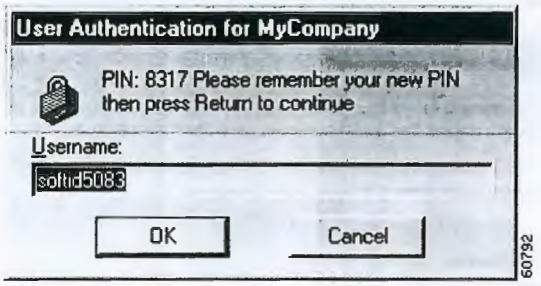
- If you responded no—the authentication program asks if you will accept a system-generated PIN. (See Figure 4-12.)

Figure 4-12 Accepting a PIN from the System



Step 2 To receive a PIN, you must respond **y** for yes and then click **OK**. When you do, the authentication program generates a PIN for you and displays it. (See Figure 4-13.) Be sure to remember your PIN.

Figure 4-13 New PIN Received



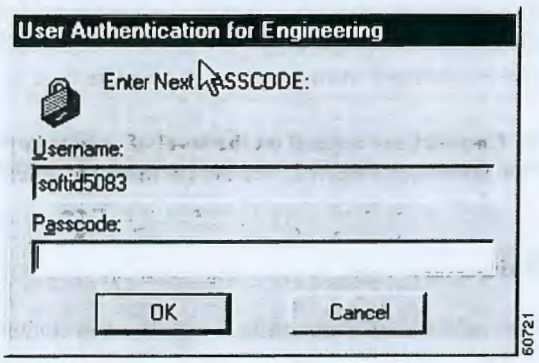
Step 3 To continue, click **OK**.

SecurID Next Cardcode Mode

Sometimes SecurID authentication prompts you to enter the next cardcode from your token card, as in Figure 4-14. SecurID displays this prompt either to resynchronize the token card with the RSA server, or because it noticed several unsuccessful attempts to authenticate with this username.

The SecurID Next Cardcode Mode dialog box might appear. (See Figure 4-14.)

Figure 4-14 Entering the Passcode for SecurID Next Card



In the Passcode field, enter the next code from your token card. This field requires only a cardcode. Do not include your PIN as part of the passcode.

Now continue to "Viewing Connection Status."

Connecting with Digital Certificates

Before you created a connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on your system. If this is not the case, then you need to obtain a digital certificate. In many cases, the network administrator of your organization can provide you with a certificate. If not, then you can obtain one by enrolling with a PKI directly using the Certificate Manager application, or you can obtain an Entrust profile through Entrust Entelligence. Currently, we support the following PKIs:

- UniCERT from Baltimore Technologies (www.baltimoretechnologies.com)
- Entrust PKI™ from Entrust Technologies (www.entrust.com)
- Versign (www.verisign.com)
- Microsoft Certificate Services in Microsoft Windows 2000 Server
- Cisco Certificate Store

The websites listed in parentheses in this list contain information about the digital certificates that each PKI provides. The easiest way to enroll in a PKI or import a certificate is to use the Certificate Manager (see "Enrolling and Managing Certificates") or Entrust Entelligence (see Entrust documentation).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 403
3698
Doc.

Note Every time you connect using a certificate, the VPN Client checks to verify that your certificate has not expired. If your certificate is within one month of expiring, the VPN Client displays a message when you attempt to connect or when you use the Properties option. The message displays the certificate common name, the "not before" date, the "not after" date, and the number of days until the certificate expires or since it has expired.

There is one exception to this rule. When you are authenticating with a Microsoft certificate, the VPN Dialer skips the automatic certificate validation process and starts the connection immediately. If there is a problem with the certificate, the connection attempt fails. To obtain information about the failure, look in the connection log file (see "Viewing and Managing the VPN Client Event Log"). To validate the certificate manually, choose Properties > Authentication > Validate Certificate.

What happens when you press **Connect** can depend on the level of private key protection on your certificate. If your certificate is password protected, you are prompted to enter the password.

Connecting with an Entrust Certificate

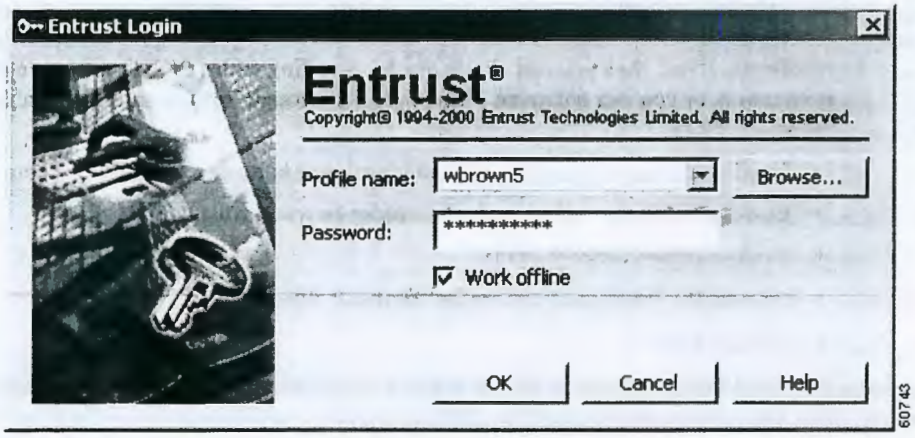
This section provides important information about what to expect when connecting with an Entrust certificate under certain conditions.

Accessing Your Profile

If you are not already logged in, you must log in to Entrust Entelligence to access your Entrust Entelligence certificate profile, using the following procedure:

After you choose **Connect** on the VPN Client main dialog box, the Entrust logon dialog box appears. (See Figure 4-15.)

Figure 4-15 Logging in to Entrust



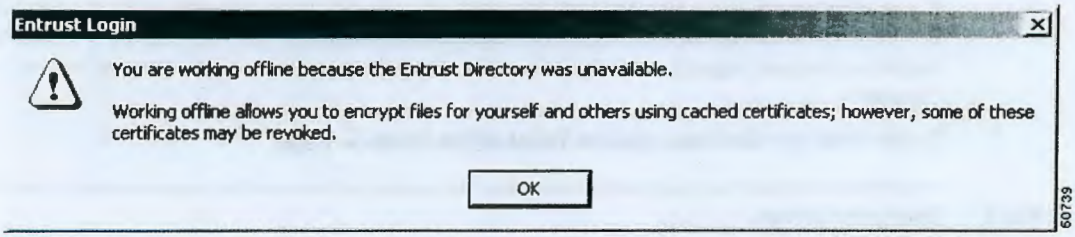
Step 1 Choose a profile name from the pull-down menu.

Your network administrator has previously configured one or more profiles for you through Entrust Entelligence. If the software is installed on your system but there are no profiles available, then you need to get a profile from your network administrator or directly through Entrust. Refer to *Entrust Entelligence Quick Start Guide* for instructions on obtaining a profile. The *VPN Client Administrator Guide* contains supplementary configuration information.

Step 2 After choosing a profile, enter your Entrust password.

Check the Work offline field to use Entrust Entelligence without connecting to the Entrust PKI. If Work offline is checked and you press **OK**, the Entrust wizard displays the message shown in Figure 4-16.

Figure 4-16 Entrust Login Message

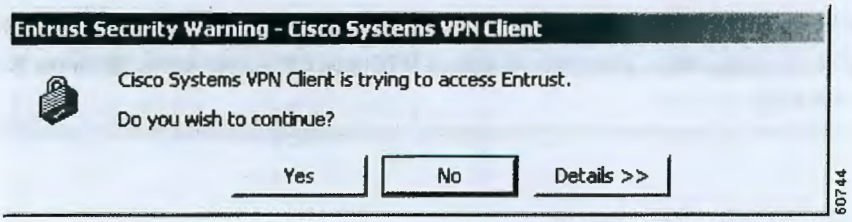


You can ignore this message. Since you are connecting to your organization's private network using an existing certificate profile, you are not interacting with the Entrust PKI. If you see this message, click **OK** to continue.

Step 3 After completing the Entrust Login dialog box (see Figure 4-15), click **OK**.

You may receive a security warning message from Entrust. This warning occurs, for example, when an application attempts to access your Entelligence profile for the first time or when you are logging in after a VPN Client software update. The message happens because Entrust wants to verify that it is acceptable for the VPN Client to access your Entrust profile.

Figure 4-17 Entrust Security Warning



Step 4 At the warning message, click **Yes** to continue.

You can now use your Entrust certificate for authenticating your new connection entry.

RQS nº 03/2005 - CN
CPMI - CORREIOS
404
Fls Nº
3698
Doc.

Entrust Inactivity Timeout

If you have a secure connection and you see a padlock next to the Entelligence icon in the Windows system tray, Entelligence has timed out. However, you have not lost your connection. If you see the Entelligence icon with an X next to it, you are logged out of Entrust, and you did not have a secure connection initially. To make a new connection, start from the beginning (see "Accessing Your Profile").

Using Entrust SignOn and Start Before Logon Together

Entrust SignOn™ is an optional Entrust application that lets you use one login and password to access Microsoft Windows and Entrust applications. This application is similar to *start before logon*, which is a VPN Client feature that enables you to dial in before logging on to Windows NT. For information about start before logon, see "Starting a Connection Before Logging on to a Windows NT Platform".

If you want to use these two features together, you should make sure you have installed Entrust Entelligence with the Entrust SignOn module before installing the VPN Client. For information about installing Entrust SignOn, refer to Entrust documentation and the *VPN Client Administrator Guide*, Chapter 1.

To use these two features together, follow these steps:

Step 1 Start your system.

When the SignOn option is installed, Entrust displays its own Ctrl Alt Delete dialog box.

Step 2 Click **Ctrl Alt Delete**.

The Entrust Options dialog box and the VPN Dialer login dialog box both pop up. The VPN Dialer dialog box is active.

Step 3 To start your VPN connection, click **Connect** on the VPN Dialer main dialog box.

The Entrust login dialog box becomes active.

Step 4 To log in to your Entrust profile, enter your Entrust password.

The VPN Dialer password prompt dialog box becomes active.

Step 5 Enter your VPN dialer username and password.

The VPN Client authenticates your credentials and optionally displays a banner and/or a notification. Respond to the banner or notification as required. Then the Windows NT logon dialog box is active.

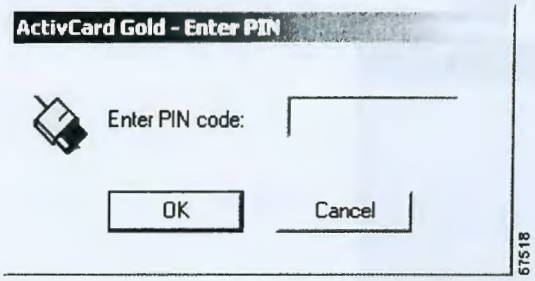
Step 6 To complete the connection, enter your Windows NT logon credentials in the Windows logon dialog box and you are done.

Connecting with a Smart Card or Token

The VPN Client supports authentication with digital certificates through a smart card or electronic token. Several vendors provide smart cards and tokens. For an up-to-date list of those that the VPN Client currently supports, see "Smart Cards Supported". Smart card support is provided through Microsoft Cryptographic API (MS CAPI). Any CryptoService provider you use must support signing with CRYPT_NOHASHOID.

Once you or your network administrator has configured a connection entry that uses a Microsoft certificate provided by a smart card, you must insert the smart card into the receptor. When you start your connection, you are prompted to enter a password or PIN, depending on the vendor. For example, Figure 4-18 shows the authentication prompt from ActivCard Gold.

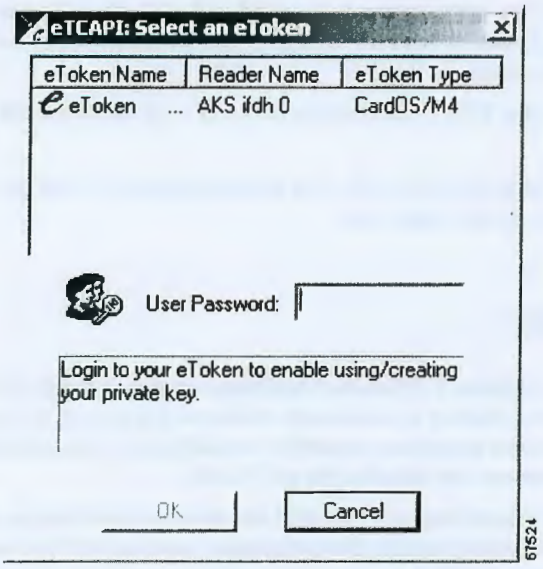
Figure 4-18 ActivCard Gold PIN Prompt



In above example, you would type your PIN code in the Enter PIN code field and click **OK**.

The next example shows how to log in to eToken from Aladdin. You select the token in the eToken Name column, type a password in the User Password field, and click **OK**.

Figure 4-19 eToken Prompt



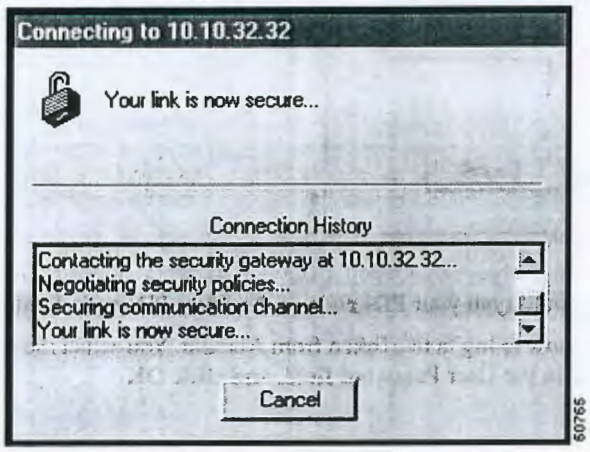
Note If your smart card or token is not inserted, the authentication program displays an error message. If this occurs, insert your smart card or token and try again.

RQS nº 03/2005 - C
CPMI – CORREIOS
405
Fls. Nº
3698
Doc.

Completing the Private Network Connection

After completing the user authentication phase, the VPN Client continues negotiating security parameters and displays a dialog box. (See Figure 4-20.) The title bar identifies the remote Cisco VPN device to which you are connecting.

Figure 4-20 Completing Connection History



If the network administrator of the Cisco VPN device has created a client banner, you see a message designated for all clients connecting to that device; for example, `The Documentation Server will be down for routine maintenance on Sunday.`

After you complete your connection, the VPN Client minimizes to an icon in the system tray on the Windows task bar.

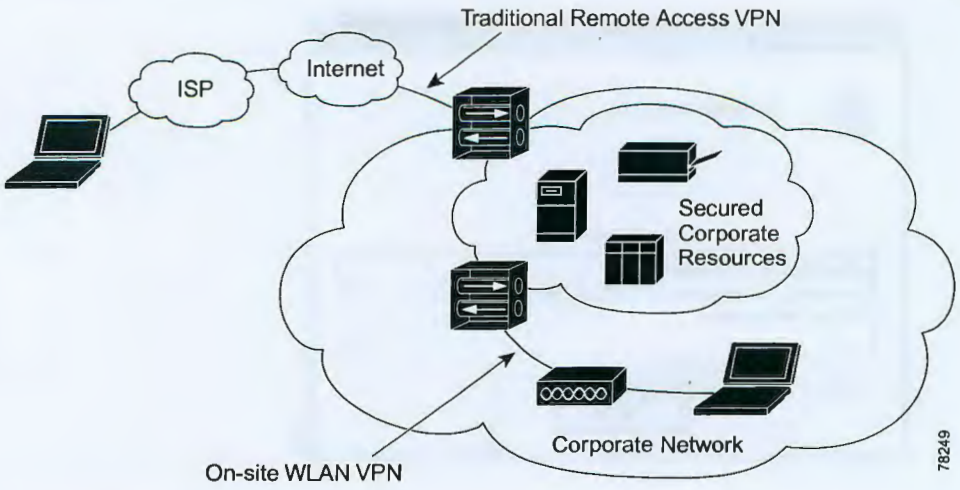
You are now connected securely to the private network via a tunnel through the Internet, and you can access the private network as if you were an onsite user.

Using Automatic VPN Initiation

Your VPN Client can automatically initiate a VPN connection based on the network to which your machine is connected. The name of this feature is called *auto initiation* for on-site Wireless LANs (WLANs). Auto initiation makes the user experience resemble a traditional wired network in which VPNs secure WLANs. These environments are also known as WLANs.

On-site WLAN VPNs are similar to remote access VPNs with an important distinction. In an on-site wireless VPN environment, enterprise administrators have deployed wireless 802.11x networks in corporate facilities and these networks use VPNs to secure the wireless part of the network link. In this case, if your PC is on a WLAN without VPN, you cannot access network resources. If a VPN exists, your access is similar to what it is with wired Ethernet connections. Figure 4-21 shows the two different types of VPN access.

Figure 4-21 Remote Access VPN Versus On-Site Wireless Access VPN



In your connection profile, your network administrator can configure a list of up to 64 matched networks (address/submasks) and corresponding connection profiles (.pcf files). When the VPN Client detects that your PC's network address matches one of the addresses in the auto initiation network list, it automatically establishes a VPN connection using the matching profile for that network.

While auto initiation is primarily for an on-site WLAN application, you can also use auto initiation in any situation based on the presence of a specific network. For example, in your home office, you may want to create an entry for your VPN to auto initiate from your corporate PC whenever you are connected to your home network, whether that network is a wireless or a wired LAN.

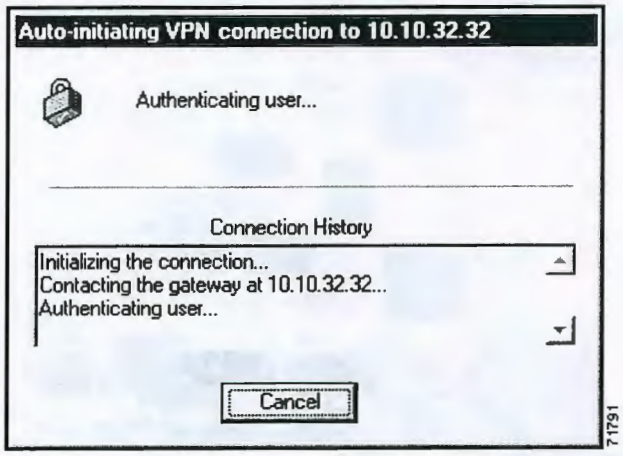
The VPN Dialer lets you know when your connection is auto initiating and informs you of various stages in the process of an auto initiated connection. You can suspend, resume, disconnect or disable auto initiation. When you disconnect or the connection attempt fails, the VPN Dialer automatically retries auto initiation using a configured interval called the retry interval. From The VPN Dialer Options menu, you can disable auto initiation, and you can change the interval between connection attempts.

Connecting Through Auto Initiation

Typically when you start your wireless system (normally a laptop), your connection initiates automatically. You do not see the VPN Dialer's main dialog. As the connection goes forward, the VPN Dialer displays the dial status screen (see Figure 4-22).

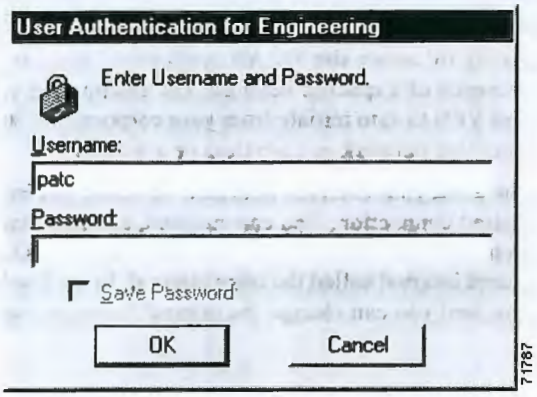
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 406
3698
Doc.

Figure 4-22 Viewing Dial Status of an Auto Initiated VPN Connection



Also, the VPN Dialer displays the authentication dialog such as the one shown in Figure 4-23.

Figure 4-23 Authenticating Auto Initialized Connection

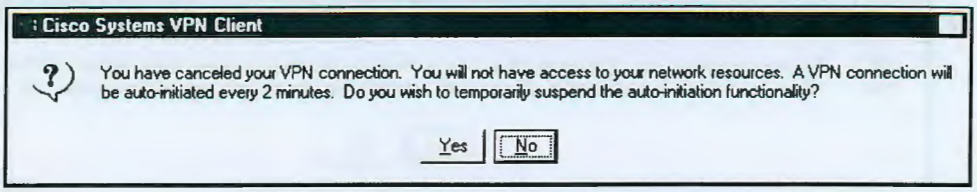


When you enter your authentication information, your connection starts immediately, as you can tell by viewing the closed yellow lock icon in the system tray.

Figure 4-24 Closed Lock—Connected

Or to cancel the connection attempt, click **Cancel** in the Dial Status dialog. When you cancel the connection attempt, the VPN Dialer displays the following message.

Figure 4-25 Canceling Connection Attempt During Authentication



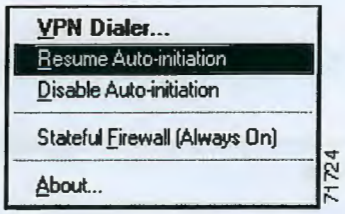
To cancel, click **No**. If you are using the Log Viewer application, in the event log, you see the message "Connection canceled."

To suspend, click **Yes**; in the event log, you see the message "Auto-initation has been suspended". When suspended, also in the task bar, you see that the yellow lock icon is now open.

Figure 4-26 Open Lock—Suspended Auto Initiation

To resume auto initiation after canceling, right-click on the open yellow lock icon and select **Resume Auto-initiation** from the menu.(See Figure 4-27).

Figure 4-27 Resuming Auto Initiation

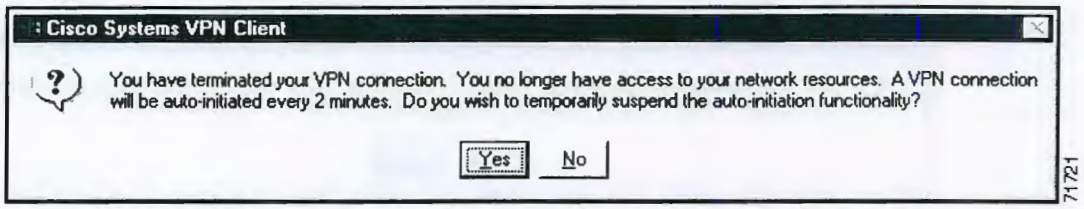


Auto initiation resumes. This is the simplest scenario of what happens during auto initiation. At various points, depending on the actions you take, you see messages, changes in the color of the icon in the system tray, and differences in choices you can make. The rest of this section describes these various alternatives.

Disconnecting Your Session

To disconnect your session, either double-click the lock icon in the system tray and click the **Disconnect** button or right-click the lock and select **Disconnect** from the menu (in the standard way). The VPN Dialer displays the following message. (See Figure 4-28.)

Figure 4-28 Disconnecting Your Session



To suspend auto initiation, click **Yes**. Auto initiation suspends until you resume it, disable it, or log off.

When you click **No**, auto initiation stays in effect and the VPN Dialer automatically retries auto initiation according to the retry interval; for example, every minute.

Changing Option Values While Auto Initiation is Suspended

When auto initiation is suspended, you can change VPN Dialer options as follows:

Step 1 Double-click yellow lock icon in the system tray.

Step 2 Click **Options**. The VPN Dialer displays the Options menu.

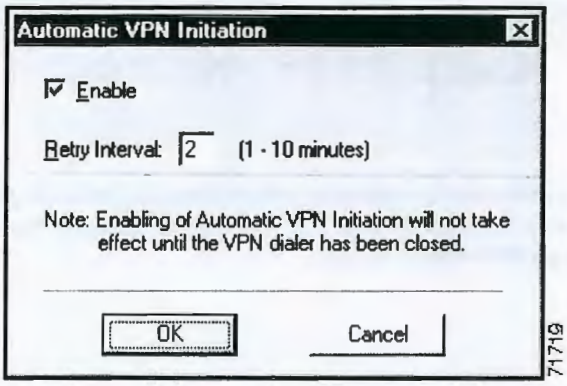
Disabling Auto Initiation

To completely shut down auto initiation, you can disable it through the Options menu by following these steps:

Step 1 Display the VPN Dialer main dialog box and click **Options**.

Step 2 Select **Automatic VPN Initiation**. The VPN Dialer displays the dialog box shown in Figure 4-29.

Figure 4-29 Setting Auto Initiation Parameters



Step 3 Click to remove the check mark from **Enable** and click **OK**. The log displays a message, "Auto-initiation has been disabled," and auto initiation terminates. When you click the dialer icon in the system tray, VPN Dialer is the only option displayed.

Note Unchecking Enable does not remove Automatic VPN Initiation option from the Options menu. This option always shows up in the menu as long as the feature has been configured by your network administrator.

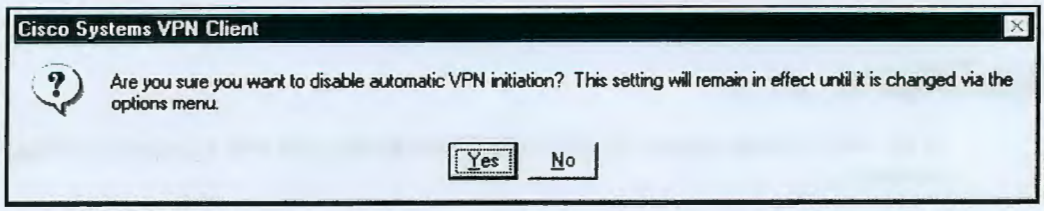
Disabling While Suspended

Alternatively, when auto initiation is suspended and you want to disable it, follow these steps:

Step 1 Right-click on the icon in the system tray.

Step 2 Select **Disable Auto-initiation**. The VPN Dialer displays a warning message (See Figure 4-30.)

Figure 4-30 Disabling an Auto Initiated Connection



Step 3 To completely disable auto initiation and eliminate further automatic retries, click **Yes**. Or to cancel the action and keep auto initiation enabled, click **No**.

Restarting After Disabling Auto Initiation

When you want to restart auto initiation, follow these steps:

Step 1 Launch the **VPN Dialer** from the Start > Programs > Cisco Systems VPN Dialer menu.

Step 2 Click **Options**.

Step 3 Select **Automatic VPN Initiation.**

Step 4 Check **Enable** and click **OK**. The log shows that auto initiation is now in effect. For an example, see Figure 4-31.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 408
3698
Doc.

Figure 4-31 Auto Initation Log Messages

```
15727 14:22:45.721 04/22/02 Sev=Info/6      DIALER/0x63300009
Auto-initiation has been suspended.

15728 16:24:25.578 04/22/02 Sev=Info/6      DIALER/0x63300009
Auto-initiation has been disabled.

15729 16:36:09.671 04/22/02 Sev=Info/6      DIALER/0x63300009
Auto-initiation has been enabled.

15730 16:36:09.671 04/22/02 Sev=Info/6      CM/0x63100036
Auto-initiation condition detected:
        Local IP 10.10.0.32
        Network 10.10.32.32
        Mask 0.0.0.0
        Connection Entry "Engineering"
```

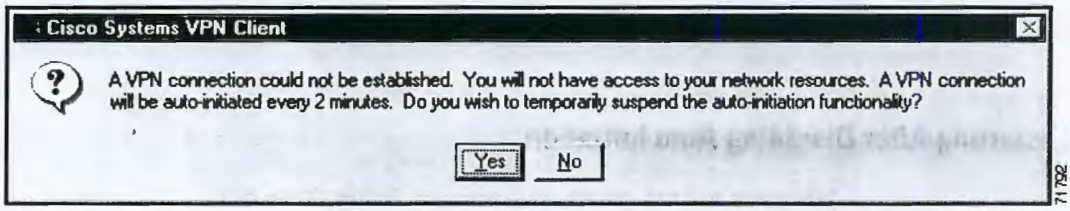
71788

Step 5 Close the VPN Dialer dialog. The Authentication dialog box displays.

Connection Failures

If the auto initiation attempt fails, the VPN Dialer notifies you with a dial status dialog and a warning message.

Figure 4-32 Auto Initiation Failure Message



To suspend auto initiation, click **Yes**. To continue retrying, click **No**. When you click No, the VPN Dialer keeps trying to connect until the connection goes through or you either disable auto initiation or log out.

Summary of Auto Initiation States

This section shows each stage of auto initiation as indicated through the changes in the appearance of the lock icon in the system tray.

Closed lock—Connected. A secure connection is in effect. Note that the closed yellow lock always indicates a secure connection whether or not you are using auto initiation.

Open yellow lock—Not connected. Auto initiation is suspended and waiting for a user action (resuming or disabling).

Open green lock—VPN Dialer is auto initiating a connection. The VPN Dialer is attempting to auto initiate from the Dial Status dialog.

Closed yellow lock with red X over it—Connection terminating. You have chosen to disconnect. The VPN Dialer asks if you want to suspend (see Figure 4-28). (Note that this icon is not specific to auto initiation but occurs any time you choose to disconnect.)

Open Blue Lock— Auto Initiation continues to be suspended with the VPN Dialer's main dialog box displaying. When you click on this lock, VPN Dialer is the only menu choice displayed. If you click **Close**, the VPN Dialer returns to the normal auto initiation suspended state.

Open Red Lock—Auto Initiation is disabling from the suspended state. VPN Dialer displays the Disable warning dialog box (see Figure 4-30) that lets you confirm or retreat.

Note Auto initiation does not connect if the VPN Dialer is opened by any means.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 403
3698
Doc.

Viewing Connection Status

The VPN Client icon on the task bar lets you view the status of your private network connection.

- Double-click the icon, or
- Click the icon with the right mouse button and choose **Status** from the pop-up menu.

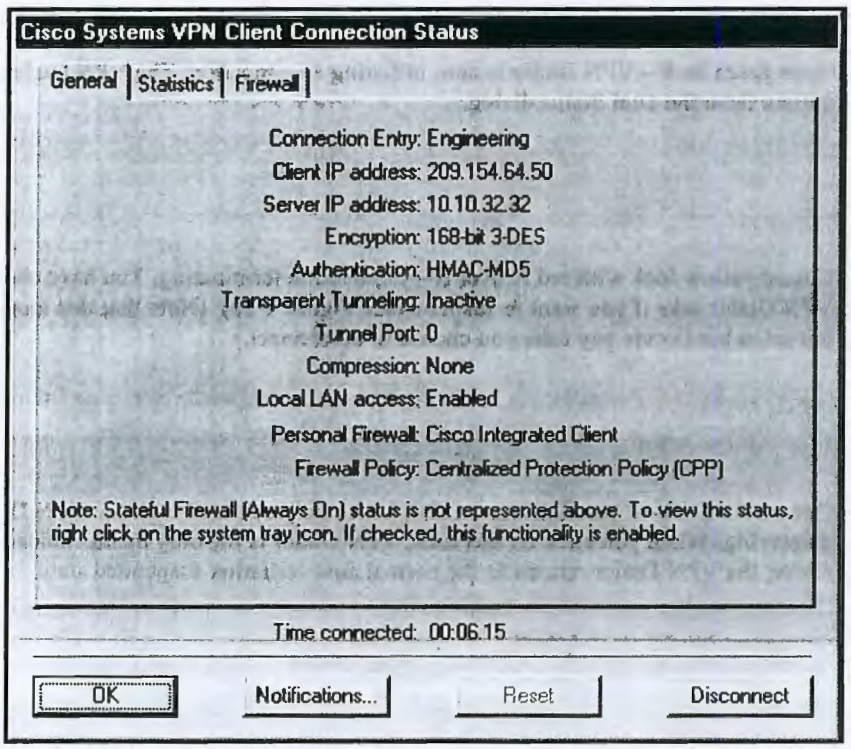
The VPN Client Connection Status dialog box appears. The dialog contains three tabs:

- General (See Figure 4-33.)
- Statistics (See Figure 4-34.)
- Firewall (See Figure 4-35).

General Information

The General tab on the Connection Status dialog box provides IP security information, listing the IPSec parameters that govern the use of this VPN tunnel to the private network.

Figure 4-33 Viewing IPSec Security Information



The parameters are the following:

- Connection Entry—The name of the profile you are using to establish the connection.
- Client IP address—The IP address assigned to the VPN Client for the current session.
- Server IP address—The IP address of the VPN device to which the VPN Client is connected.

ECT 2007 CPL AC

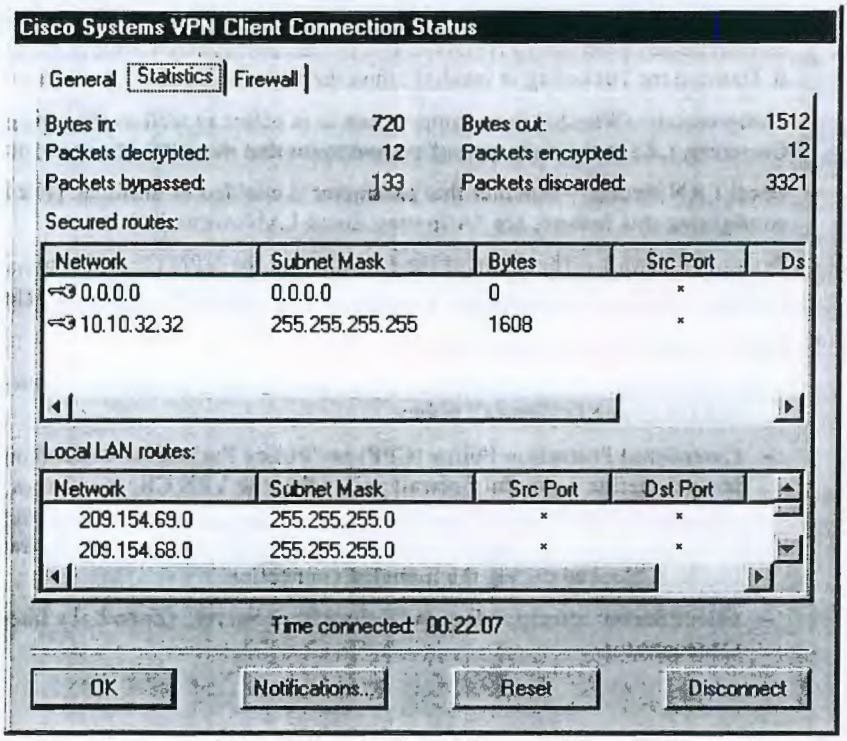
- Encryption—The data encryption method for traffic through this tunnel. Encryption makes data unreadable if intercepted.
- Authentication—The data, or packet, authentication method used for traffic through this tunnel. Authentication verifies that no one has tampered with data.
- Transparent Tunneling—The status of tunnel transparent mode in the client, either active or inactive.
- Tunnel Port—If Transparent Mode is active, the tunnel port through which packets are passing. This field also identifies whether the VPN Client is sending packets through UDP or TCP. This port number comes from the VPN device. If UDP, the port is negotiated; if TCP the port is preconfigured. If Transparent Tunneling is inactive, then the value of Tunnel Port is zero.
- Compression—Whether data compression is in effect as well as the type of compression in use. Currently, LZS is the only type of compression that the VPN Client supports.
- Local LAN Access—Whether this parameter is enabled or disabled. (For information on configuring this feature, see "Allowing Local LAN Access".)
- Personal Firewall—The name of the firewall that the VPN Client is enforcing, such as the Cisco Integrated Client, Zone Labs ZoneAlarm, ZoneAlarm Pro, BlackICE Defender, and so on.
- Firewall Policy—The firewall policy in use:
  - AYT (Are You There) enforces the use of a specific personal firewall but does not require you to have a specific firewall policy.
  - Centralized Protection Policy (CPP) or "Policy Pushed" as defined on the VPN Concentrator lets you define a stateful firewall policy that the VPN Client enforces for Internet traffic while a tunnel is in effect. CPP is for use during split tunneling and is not relevant for a tunnel everything configuration. In a tunnel everything configuration, all traffic other than tunneled traffic is blocked during the tunneled connection.
  - Client/Server corresponding to "Policy from Server" (Zone Labs Integrity) on the VPN Concentrator

RQS nº 03/2003
CPMI - CORREIOS
Fls. Nº 410
3698
Doc.

Statistics

The Statistics tab on the Connection Status dialog box shows statistics for data packets that the VPN Client has processed during the current session or since the statistics were reset. Reset affects only this tab.

Figure 4-34 Viewing Statistics



- Bytes in—The total amount of data received after a secure packet has been successfully decrypted.
- Bytes out—The total amount of encrypted data transmitted through the tunnel.
- Packets decrypted—The total number of data packets received on the port.
- Packets encrypted—The total number of secured data packets transmitted out the port.
- Packets bypassed—The total number of data packets that the VPN Client did not process because they did not need to be encrypted. Local ARPs and DHCP fall into this category.
- Packets discarded—The total number of data packets that the VPN Client rejected because they did not come from the secure VPN device gateway.

Secured Routes

The Secured Routes section lists the IPSec Security Associations (SAs).

In Figure 4-34 under Secured Routes, the columns show the following types of information.

- Key icon—In the first row, you see a key icon at the start of the connection entry. This key shows that the route is secure. The software generates a key as soon as the client needs to send secure data through the tunnel to the networks on the other side. The absence of a key means that the SA is no longer active. The SA may have timed out due to inactivity. Sending data to this network re-establishes the SA, and the key reappears.
- Network—The IP address of the remote private network with which this VPN Client has an SA.
- Subnet Mask—The subnet mask of the IP address for this SA.
- Bytes—The total amount of data this SA has processed. This includes data before encryption as well as encrypted data received.
- Src Port, Dst Port, and Protocol are for future use.

Local LAN Routes

If active the Local LAN Routes box shows the network addresses of the networks you can access on your local LAN while you are connected to your organization's private network through an IPSec tunnel. You can access up to 10 networks on the client side of the connection. A network administrator at the central site must configure the networks you can access from the client side. For information on configuring Local LAN Access on the VPN 3000 Concentrator, refer to *VPN Client Administrator Guide*, Chapter 1.

Time Connected

The Statistics tab also displays the time in days, hours, minutes and seconds, that has elapsed since you initiated the connection.

Firewall Tab

The Firewall tab displays information about the VPN Client's firewall configuration.

The VPN Concentrator's network manager sets up the firewall policy under Configuration | User Management | Base Group or Group | Client FW tab. There are three options:

- Are You There—The supported personal firewall software on the VPN Client PC controls its own rules. The VPN Client polls the firewall every 30 seconds to make sure it is still running, but does not confirm that a specific policy is enforced.
- Centralized Protection Policy—This policy takes advantage of the Cisco Integrated Client. The policy rules are defined on the VPN Concentrator and sent to the VPN Client during each connection attempt. The VPN Client enforces these rules for all non-tunneled traffic while the tunnel is active.
- Client/Server—This policy relates to Zone Labs Integrity solution. The policy is defined on the Integrity Server in the private network and sent to the VPN Concentrator, which in turns sends it to the Integrity Agent on the VPN Client PC to implement. Since Integrity is a fully functional personal firewall, it can intelligently decide on network traffic based on applications as well as data.

RQS nº 03/2005 - CN
CPMI - CORREIOS
411
Fls. Nº
Doc.

Note CPP affects Internet traffic only. Traffic across the tunnel is unaffected by its policy rules. If you are operating in tunnel everything mode, enabling CPP has no affect.

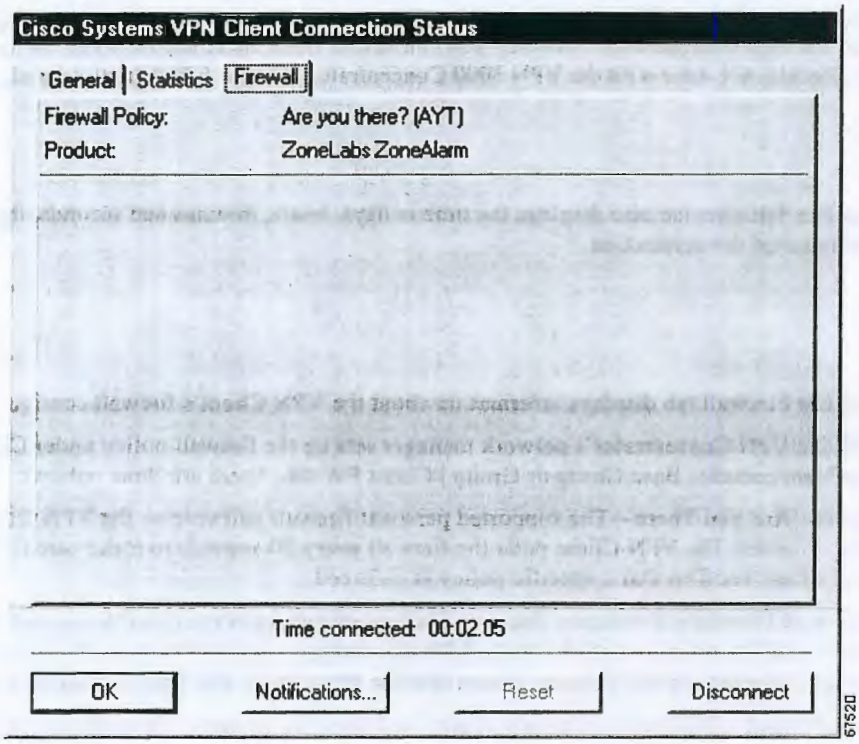
The information shown on this tab varies according to your firewall policy.

- AYT—When the Are You there (AYT) is the supported capability, the Firewall tab shows only the firewall policy (AYT) and the name of the firewall product (see Figure 4-35).
- Centralized Protection Policy (CPP)—When CPP is the supported capability, the Firewall tab includes the firewall policy, the firewall in use, and firewall rules (see Figure 4-36).
- Client/Server—When the Client/Server is the supported capability, the Firewall tab displays the firewall policy as Client/Server, the name of the product as ZoneLabs Integrity Agent, the user ID, session ID, and the addresses and port numbers of the firewall servers (see Figure 4-37).

AYT Firewall Tab

The Firewall tab shows that AYT is running and displays the name of the firewall product that supports AYT.

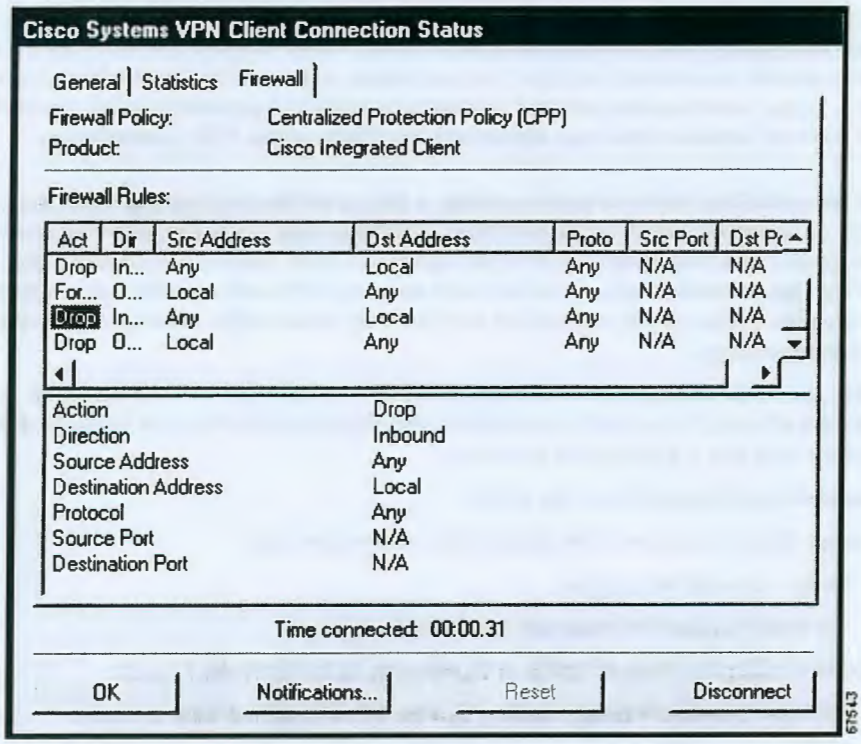
Figure 4-35 Firewall Tab for AYT capability



Centralized Protection Policy (CPP) Using the Cisco Integrated Client

CPP is a stateful firewall policy that is defined on and controlled from the VPN Concentrator. It can add protection for the VPN Client PC and private network from intrusion when split tunneling is in use. For CPP (see Figure 4-36), the Firewall tab shows you the firewall rules in effect.

Figure 4-36 Firewall Tab for CPP



This status screen lists the following information:

- Firewall Policy—The policy established on the VPN Concentrator for this VPN Client.
- Product—Lists the name of the firewall currently in use, such as Cisco Integrated Client, Zone Alarm Pro, and so on.

Firewall Rules

The Firewall Rules section shows all of the firewall rules currently in effect on the VPN Client. Rules are in order of importance from highest to lowest level. The rules at the top of the table allow inbound and outbound traffic between the VPN Client and the secure gateway and between the VPN Client and the private networks with which it communicates. For example, there are two rules in effect for each private network that the VPN Client connects to through a tunnel (one rule that allows traffic outbound and another that allows traffic inbound). These rules are part of the VPN Client software. Since they are at the top of the table, the VPN Client enforces them before examining CPP rules. This approach lets the traffic flow to and from private networks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
412
Fls. Nº
3698
Doc.

CPP rules (defined on the VPN Concentrator) are only for nontunneled traffic and appear next in the table. For information on configuring filters and rules for CPP, see *VPN Client Administrator Guide,* Chapter 1. A default rule "Firewall Filter for VPN Client (Default)" on the VPN Concentrator lets the VPN Client send any data out, but permits return traffic in response only to outbound traffic.

Finally, there are two rules listed at the bottom of the table. These rules, defined on the VPN Concentrator, specify the filter's default action, either drop or forward. If not changed, the default action is drop. These rules are used only if the traffic does not match any of the preceding rules in the table.

Note The Cisco Integrated Client firewall is stateful in nature, where the protocols TCP, UDP, and ICMP allow inbound responses to outbound packets. For exceptions, refer to *VPN Client Administrator Guide*, Chapter 1. If you want to allow inbound responses to outbound packets for other protocols, such as HTTP, a network administrator must define specific filters on the VPN Concentrator.

You can move the bars on the column headings at the top of the box to expand their size; for example, to display the complete words Action and Direction rather than Act or Dir. However, each time you exit from the display and then open this status tab again, you must expand the columns again. Default rules on the VPN Concentrator (drop any inbound and drop any outbound) are always at the bottom of the list. These two rules act as a safety net and are in effect only when traffic does not match any of the rules higher in the hierarchy.

To display the fields of a specific rule, click on the first column and observe the fields in the next area below the list of rules. For example, the window section underneath the rules in Figure 4-36 displays the fields for the rule that is highlighted in the list.

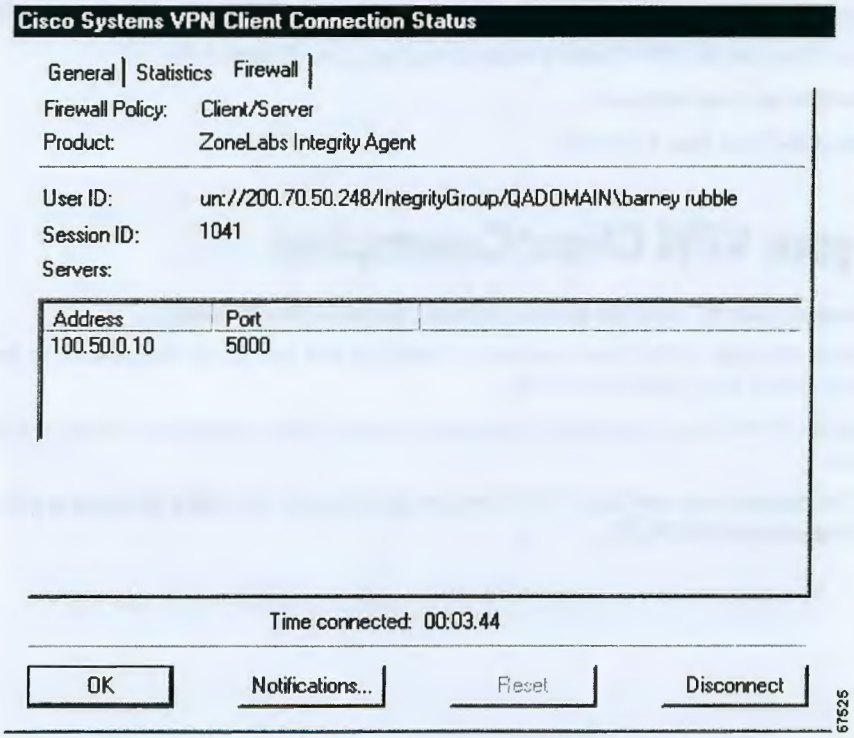
A firewall rule includes the following fields:

- Action—The action taken if the data traffic matches the rule:
  - Drop = Discard the session.
  - Forward = Allow the session to go through.
- Direction—The direction of traffic to be affected by the firewall:
  - Inbound = traffic coming into the PC, also called local machine.
  - Outbound = traffic going out from the PC to all networks while the VPN Client is connected to a secure gateway.
- Source Address—The address of the traffic that this rule affects:
  - Any = all traffic; for example, drop any inbound traffic.
  - This field can also contain a specific IP address and subnet mask.
  - Local = the local machine; if the direction is Outbound then the Source Address is local.
- Destination Address—The packet's destination address that this rule checks (the address of the recipient).
  - Any = all traffic; for example, forward any outbound traffic.
  - Local = The local machine; if the direction is Inbound, the Destination Address is local.
- Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP and so on).
- Source Port—Source port used by TCP or UDP.
- Destination Port—Destination port used by TCP or UDP.

Client/Server Firewall Tab

When Client/Server is the supported policy, the Firewall tab displays the name of the firewall policy, the name of the product, the user ID, session ID, and the addresses and port numbers of the firewall servers in the private network (see Figure 4-37). Zone Labs Integrity is a Client/Server firewall solution in which the Integrity Server (IS) acts as the firewall server that pushes firewall policy to the Integrity Agent (IA) residing on the VPN Client PC. Zone Labs Integrity can also provide a centrally controlled always on personal firewall.

Figure 4-37 Client/Server Firewall Tab



Firewall Policy—This field shows that Client/Server is the supported policy.

Product—Lists the name of the Client/Server solution currently in use, such as Zone Labs Integrity Client.

User ID—In the format *xx://IP address of the VPN Concentrator/group name and user name*

Where: *xx* can be **un** or **dn**:

un = The gateway-based ID is based on the group and user name.

dn = The gateway-based ID is based on the distinguished name (as is the case when using digital certificates).

The User ID is used to initialize the firewall client.

Session ID—The session ID of the connection between all of the entities. This is used to initialize the firewall client and is helpful for troubleshooting.

Servers—The IP address and port number of each firewall server. For Release 3.6, there is only one.

RQS nº 03/2005
CPMI - CORREIOS
Fls. Nº 413
Doc. 3698

Resetting Statistics

To reset all connection statistics to zero, click **Reset**. *There is no undo.* Reset affects only the connection statistics, not the other sections of this dialog box.

Closing the VPN Client

You may want to close the VPN Client when it is running on your PC but not connected to a remote network.

To close the VPN Client when it is not connected to a remote network, do one of the following:

- Click **Close** on the VPN Dialer's main dialog box. (See Figure 4-1).
- Press **Esc** on your keyboard.
- Press **Alt-F4** on your keyboard.

Disconnecting your VPN Client Connection

To disconnect your PC from the private network, do one of the following:

- Double-click the VPN Client icon on the Windows task bar. Click **Disconnect** on the Connection Status dialog box. (See Figure 4-33.)
- Click the VPN Client icon with the secondary mouse button and choose **Disconnect** from the pop-up menu.

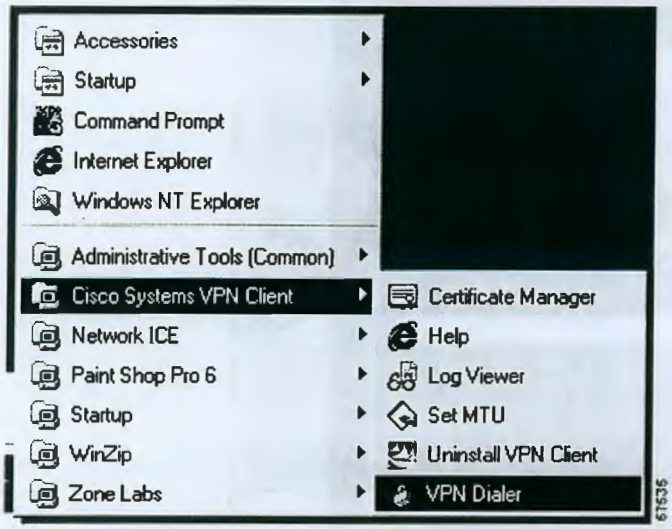
Your IPSec session ends and the VPN Client closes. You must manually disconnect your dial-up networking connection (DUN).

CHAPTER 5

Managing the VPN Client

This chapter explains the tasks you can perform to manage connection entries, view and manage event reporting, and upgrade or uninstall the VPN Client software. The management features are available from the Cisco Systems VPN Client applications menu. (See Figure 5-1.)

Figure 5-1 Cisco Systems VPN Client Menu of Applications



Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

This chapter includes the following sections:

- Managing VPN Client Connection Entries
- Enabling Stateful Firewall (Always On)
- Launching an Application
- Managing Windows NT Logon Properties
- Viewing and Managing the VPN Client Event Log
- Receiving Notifications From a VPN Device

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 414
3698
Doc.

- Upgrading the VPN Client Software (InstallShield)
- Uninstalling the VPN Client with the Uninstall Application

To configure properties of connection entries, see "Configuring the VPN Client."

Note If you are a system administrator, refer to the *VPN Client Administrator Guide* for information on configuring the VPN 3000 Concentrator and preparing preconfigured profiles for VPN Client users.

Managing VPN Client Connection Entries

To manage a connection entry, start the Cisco VPN Client and choose **VPN Dialer** from the menu of applications.

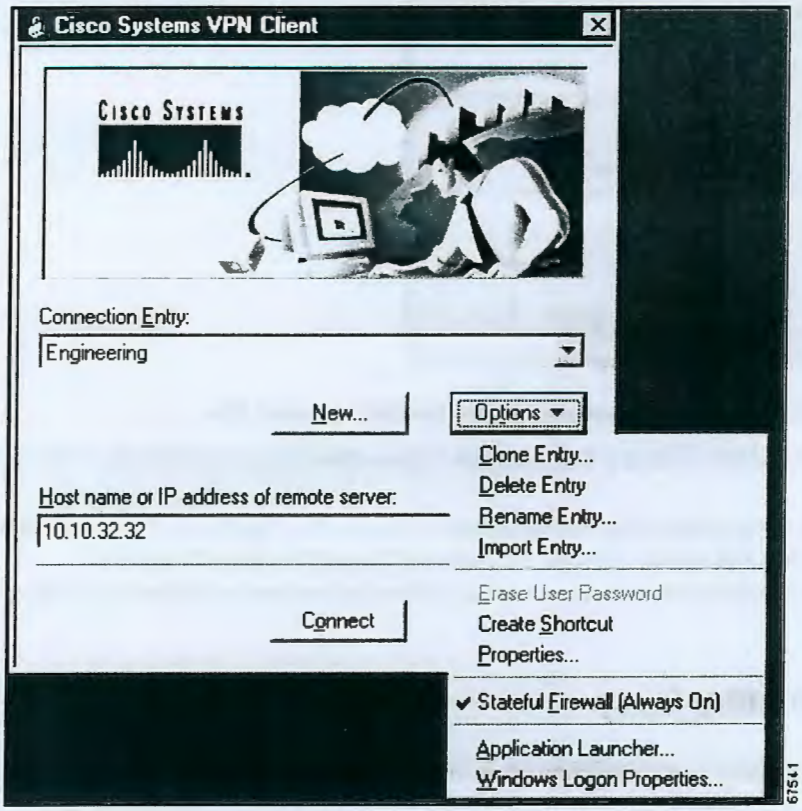
The VPN Client main dialog box appears. (See Figure 5-2.)

Figure 5-2 VPN Client Main Dialog Box (VPN Dialer)

Click the **Connection Entry** drop-down menu arrow and choose an entry.

Click **Options** to display the menu.

Figure 5-3 VPN Client Options Menu



Note On a Windows 9x, Windows Me, or Windows XP home system, the VPN Client does not display Windows Logon Properties.

Cloning a Connection Entry

To clone a connection entry with all its properties and use it as the basis for creating a new entry, follow these steps:

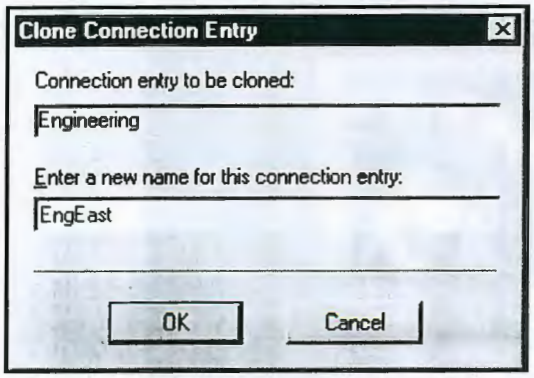
Step 1 On the VPN Client's main dialog box, click the Connection Entry drop-down menu and choose the entry you want to clone.

Step 2 On the VPN Client Options menu, choose **Clone Entry**. (See Figure 5-3.)

The Clone Connection Entry dialog box appears. (See Figure 5-4.)

RQS nº 03/200
CPMI - CORREIOS
Fls. Nº 415
3694
Doc.

Figure 5-4 Clone Connection Entry Dialog Box



Step 3 Enter a name for the new connection entry in the field and click **OK**.

Step 4 The dialog box closes. The new name appears in the Connection Entry list in the VPN Client main dialog box.

Step 5 To configure the properties of this new connection entry, click **Options > Properties** on the VPN Client main dialog box and see the "Setting or Changing Connection Entry Properties".

Deleting a Connection Entry

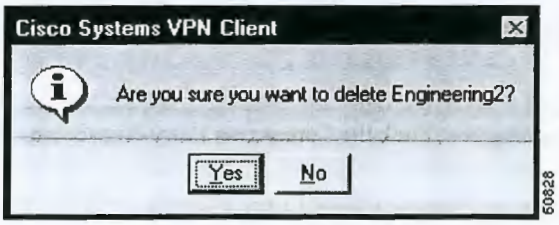
To delete a configured connection entry, follow these steps:

Step 1 On the VPN Client's main dialog box, click the Connection Entry drop-down menu arrow and choose the entry you want to delete.

Step 2 On the VPN Client Options menu, choose **Delete entry**. (See Figure 5-3.)

A confirmation dialog box appears. (See Figure 5-5.)

Figure 5-5 Confirming Deletion of a Connection Entry



Step 3 Click **Yes** or **No**:

- To permanently delete the connection entry, click **Yes**. *There is no undo.*
- To retain the connection entry, click **No**.

The VPN Client returns to its main dialog box.

Renaming a Connection Entry

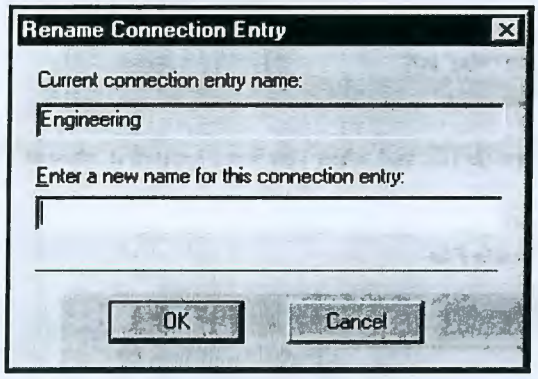
You can rename a connection entry and retain all its properties. Each connection entry name must be unique. Since these names are *not* case-sensitive, be sure the new name differs in content, not just case.

Step 1 On the VPN Client's main dialog box, click the Connection Entry drop-down menu and choose the entry you want to rename.

Step 2 On the VPN Client Options menu, choose **Rename Entry**. (See Figure 5-3.)

The Rename Connection Entry dialog box appears. (See Figure 5-6.)

Figure 5-6 Entering a New Name for a Connection Entry



Step 3 Enter a new name for this connection entry in the field and click **OK**.

The dialog box closes. The new name appears in the Connection Entry list in the VPN Client main dialog box.

Importing a VPN Client Configuration File

You can automatically configure your VPN Client with new settings by importing a new configuration file (a file with a .pcf extension, called a profile) that your system administrator supplies.

To automatically configure a VPN Client, perform the following steps:

Step 1 Obtain a new VPN Client profile (`.pcf`) file from your system administrator.

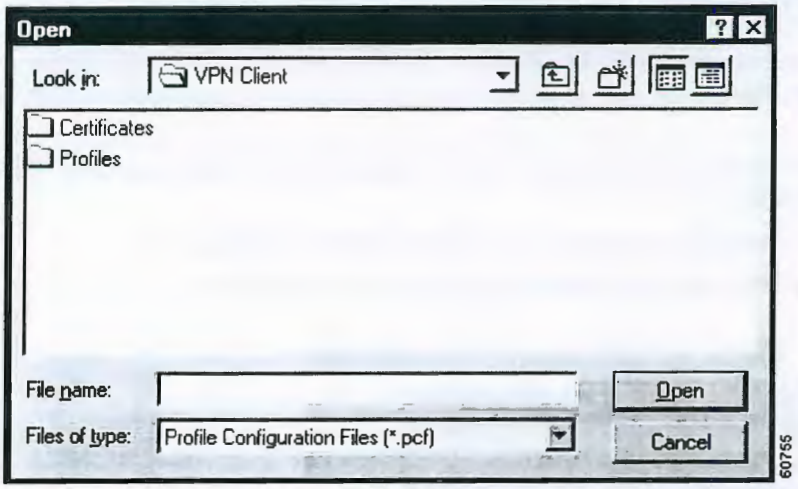
Step 2 Load the file on your hard disk.

Step 3 On the VPN Client main dialog box, click **Options** and choose **Import Entry** from the menu.

The VPN Client opens a window for you to choose the profile file. (See Figure 5-7.)

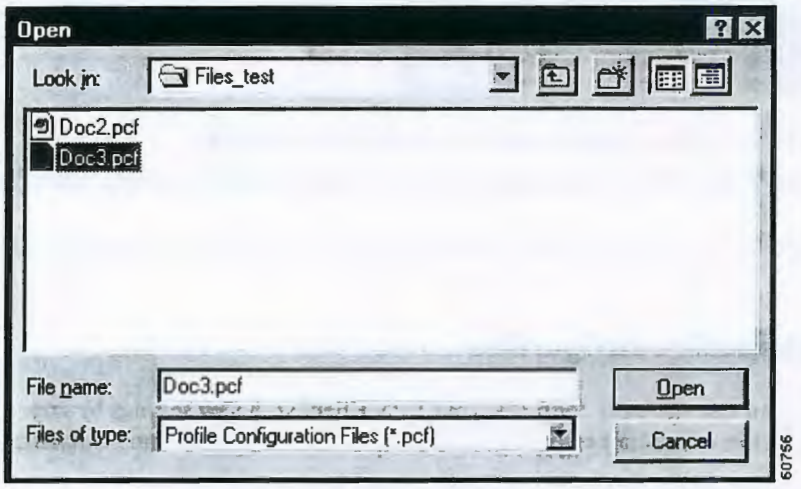
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 416
Doc.

Figure 5-7 Choosing a File to Import



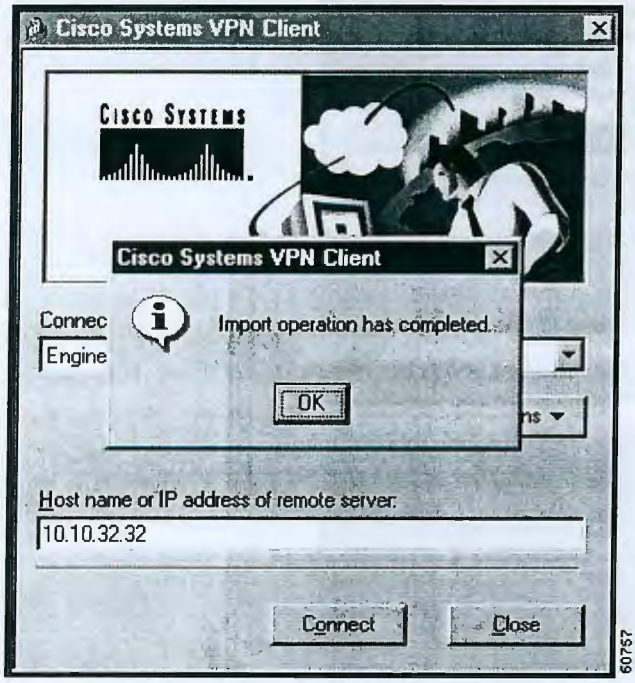
Step 4 Browse until you locate the profile file and when you have located it, choose it and click **Open**. (See Figure 5-8.)

Figure 5-8 Importing the Profile File



The VPN Client displays a message informing you that your file import was successful. (See Figure 5-9.) If the profile already exists, you receive a message asking if you want to overwrite it.

Figure 5-9 Import Successful



Step 5 To continue, click **OK**.

Alternatively, you can copy the .pcf file into the Profiles directory and restart the VPN Dialer application.

Your VPN Client is now configured with the connection entries and parameters specified by this new profile file. You can examine or modify the connection entries by clicking the Connection Entry drop-down menu on the main dialog box, choosing an entry, and clicking **Options > Properties**.

Erasing a Saved Password for a Connection Entry

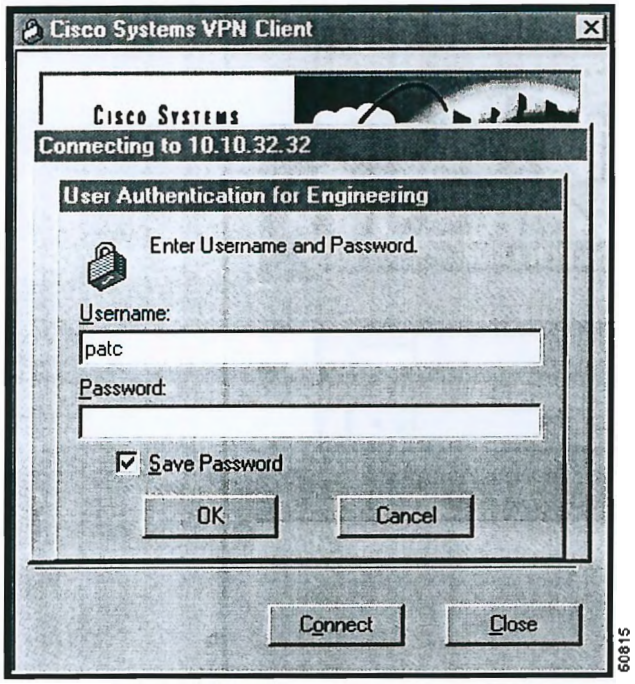
You or your administrator may have configured an entry to save the authentication password on your PC so you do not have to enter a password when you are connecting to the VPN device. Normally we recommend that you not use this feature, because storing the password on the PC can compromise security, and requiring a password to authenticate you every time you attempt to connect to the VPN device is fundamental to maintaining security on the private network. However, there may be reasons for temporarily bypassing the authentication dialog box, for example, when you want to create a batch file for your PC to log in to a VPN device to accomplish some task that requires using the private network behind the VPN device.

If there is a password saved on your system, and authentication fails, your password might be invalid.

To eliminate a saved password, use the Erase User Password feature on the Options menu. Erase User Password is available only when you have previously checked Save Password on the User Authentication dialog box. (See Figure 5-10.)

ECTI CPL-AC
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 417
Doc. 3698

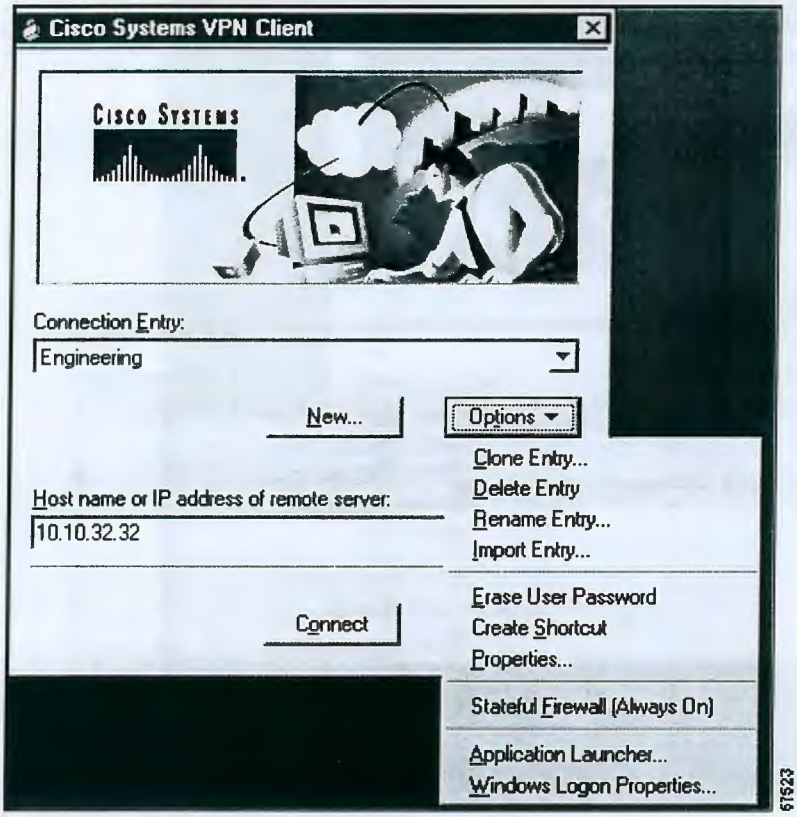
Figure 5-10 Saving Password During Authentication



When the VPN device allows saving passwords on the remote site and Save Password is in effect, then Erase User Password is available on the Options menu. (See Figure 5-11.)

Note If you get a failed-to-authenticate message, you should enable **Erase User Password** on the VPN Client and verify that your password is valid. When you attempt to connect, the VPN Client prompts you to enter your password.

Figure 5-11 Erase User Password Available

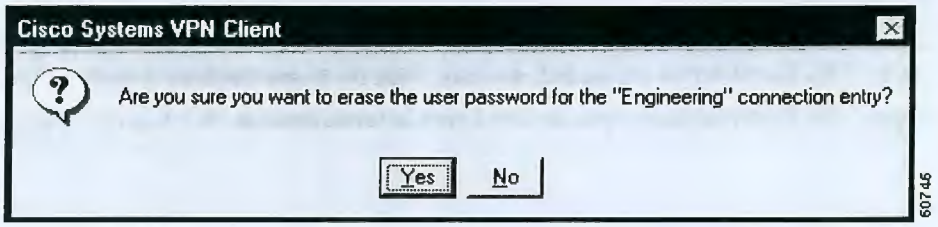


Note The VPN Client displays Windows Logon Properties only on Windows NT, Windows 2000, and Windows XP.

To enable this feature, click **Erase User Password**.

The VPN Client prompts you to confirm (See Figure 5-12.)

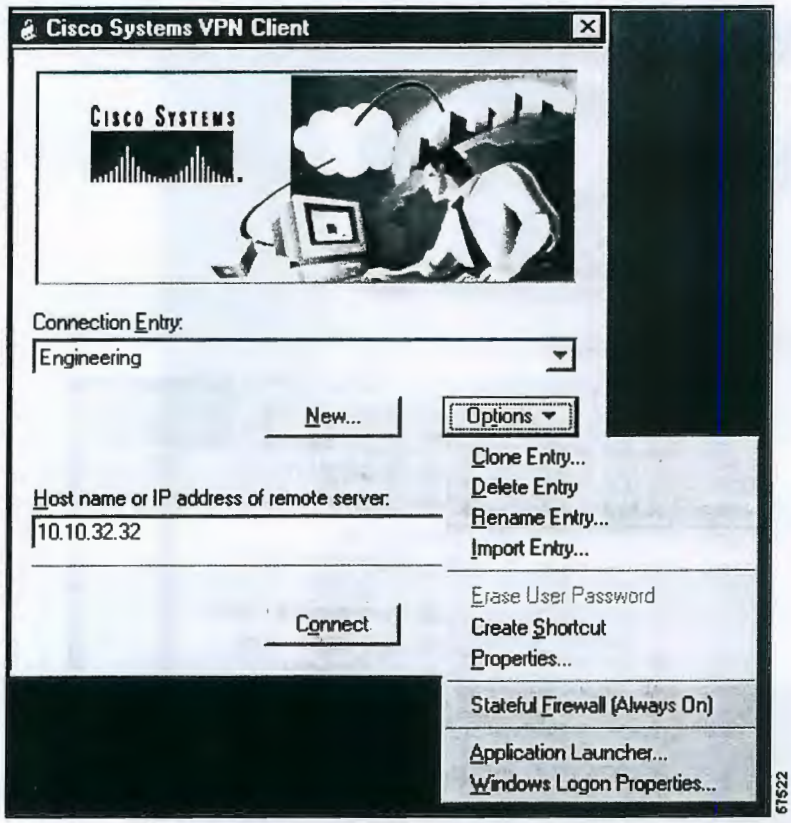
Figure 5-12 Verifying Erase User Password



With Erase User Password in effect, the next time you connect, the authentication dialog box prompts you to enter your password: on the Options menu, the Erase User Password feature is no longer available. (See Figure 5-13.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 418
3698
Doc.

Figure 5-13 Erase User Password Unavailable



Note The VPN Client displays Windows Logon Properties only on Windows NT, Windows 2000, and Windows XP.

Creating a Shortcut for a Connection Entry

You can create a shortcut on your desktop to quickly and directly launch a VPN Client connection entry that you use frequently.

Step 1 On the VPN Client's main dialog box, click the **Connection Entry** drop-down menu and choose an entry.

Step 2 On the VPN Client Options menu, choose **Create Shortcut**. (See Figure 5-3.)

The shortcut appears on your desktop, as in this example. (See Figure 5-14.)

Figure 5-14 Connection Entry Shortcut

The VPN Client main dialog box remains open.

Enabling Stateful Firewall (Always On)

The VPN Client includes an integrated stateful firewall that provides protection when split tunneling is in effect and protects the VPN Client PC from Internet attacks while the VPN Client is connected to a VPN Concentrator through an IPSec tunnel. This integrated firewall includes a feature called Stateful Firewall (Always On).

Stateful Firewall (Always On) provides even tighter security. When enabled, this feature allows *no* inbound sessions from all networks, whether or not a VPN connection is in effect. Also, the firewall is active for both encrypted and non encrypted traffic. There are two exceptions to this rule. The first is DHCP, which sends requests to the DHCP server out one port but receives responses from DHCP through a different port. For DHCP, the stateful firewall allows inbound traffic. The second is ESP. The stateful firewall allows ESP traffic from the secure gateway, because ESP rules are packet filters and not session-based filters. For the latest information on other exceptions, if any, refer to *Release Notes for Cisco VPN Client for Windows*.

To enable the stateful firewall, click **Stateful Firewall (Always on)** on the Options menu. When Stateful Firewall (Always On) is enabled, you see a check in front of the option. This feature is disabled by default. You can enable or disable this feature from the VPN Client Options menu. During a VPN connection, you can view the status of this feature by right-clicking the lock icon in the system tray. You can also enable or disable this feature from the same menu.

Launching an Application

You can configure the dialer to automatically launch an application before establishing a connection. Some examples of why you would want to use this feature follow:

- You are configured for start before logon and you need to start an authentication application at the logon desktop.
- You want to launch a monitoring application such as the Log Viewer before each connection. (See Figure 5-15 to Figure 5-17.)

To configure the VPN Dialer to launch an application from the logon desktop, use the Application Launcher.

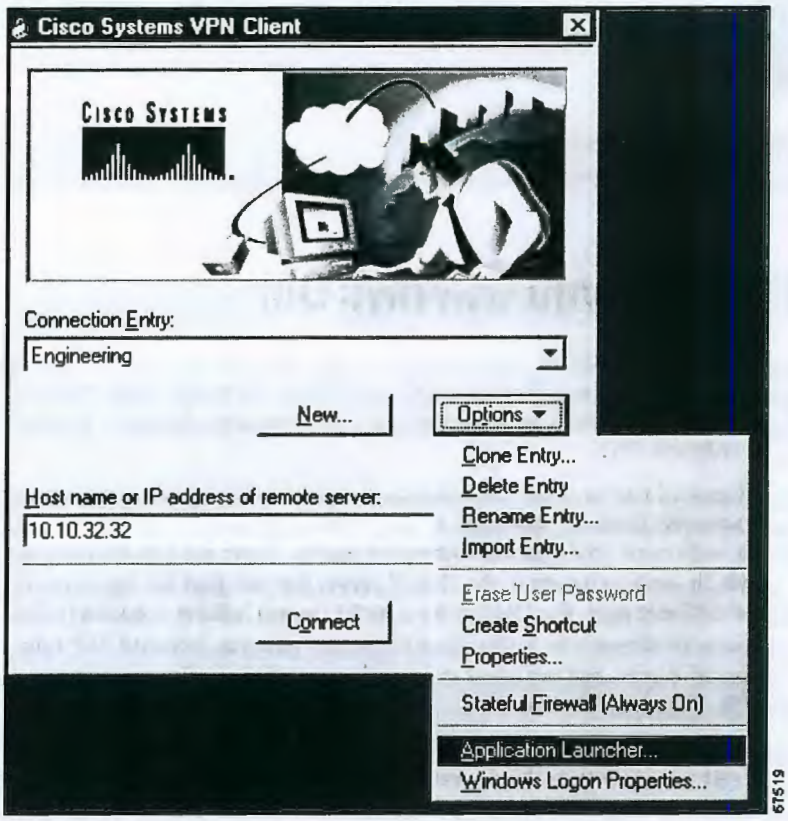
The Application Launcher starts the specified application once per session. To launch an application again, you must exit from the VPN Dialer, restart the VPN Dialer, and launch the application.

RQS nº 03/200
CPMI - CORREIOS
Fls. Nº 419
3698
Doc.

To activate Application Launcher, follow these steps:

Step 1 Open the VPN Dialer Options pull-down menu (shown in Figure 5-3) and click **Application Launcher.** (See Figure 5-15.)

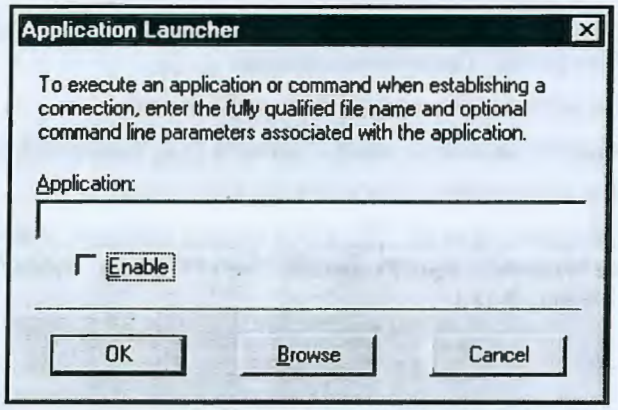
Figure 5-15 Application Launcher Option



Note The VPN Client displays Windows Logon Properties only on Windows NT, Windows 2000, and Windows XP.

The VPN Dialer displays a dialog box prompting for the name of the application. (See Figure 5-16.)

Figure 5-16 Entering the Name of the Application



Step 2 Click **Browse** to locate and then choose the complete pathname to the application as well as the name of the application. (See Figure 5-17.)

The application name appears in the Application Launcher dialog box. In this example, the VPN Dialer is configured to launch the Log Viewer before a connection.

Figure 5-17 Choosing an Application

Step 3 Click **Enable** and then click **OK**.

Turning Off Application Launcher

To disable Application Launcher, follow these steps:

Step 1 Open the Options pull-down menu and choose **Application Launcher**.

Step 2 When the Application Launcher dialog box displays, clear the Enable checkbox.

RQS nº 03/2005
CPMI - CORREIOS
Fls. Nº 420
3698
Doc.

Managing Windows NT Logon Properties

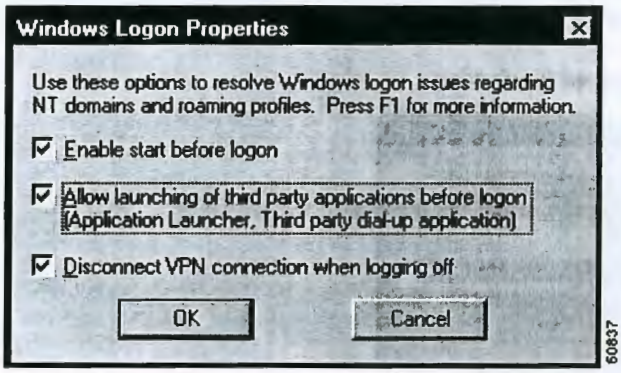
This section describes special logon features for the Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP. These features include:

- Ability to start a connection before logging on to a Windows NT system
- Permission to launch a third party application before logging on to a Windows NT system
- Control over auto-disconnect when logging off of a Windows NT system

To access the Windows logon properties, open the VPN Client Options pull-down menu (shown in Figure 5-3) and choose **Windows Logon Properties**. The VPN Client displays a dialog box containing three parameters. (See Figure 5-18.)

Note The VPN Client displays Windows Logon Properties only on Windows NT, Windows 2000, and Windows XP.

Figure 5-18 Windows Logon Properties



Starting a Connection Before Logging on to a Windows NT Platform

On a Windows NT platform, you can connect to the private network before you log on to your system. This feature is called *start before logon* and its purpose is primarily to let you log in to the domain and run login scripts.

Your administrator may have set this up for you. Once you establish a VPN connection, your credentials are sent to a domain controller for logging in to your system. If you need to launch an application before you log on, see the section "Launching an Application" for information.

When you have established a successful VPN connection, the VPN Dialer window closes, and your logon window displays. If the connection is not successful, the VPN Dialer window continues to display. Your administrator may have set up a banner that lets you know when you have a successful connection.

To activate this feature, follow these steps:

Step 1 Open the VPN Client Options pull-down menu (shown in Figure 5-3) and choose **Windows Logon Properties**.

Step 2 Check **Enable start before logon** and then click OK. (See Figure 5-18.)

What Happens When You Use Start Before Logon

When start before logon is active, the following events occur when your system starts:

- Your system logon dialog box displays. Other messages might display as well, depending on your setup. Wait until you see the VPN Dialer start.
- The VPN Dialer starts and displays the connection dialog box over the system logon dialog box.
- You establish your connection to the private network of the VPN Device.
- You log on to your system.

Note You can use certificates for authentication with start before logon when your personal certificate, along with the CA or intermediary certificate(s), are in your Cisco certificate store and the Microsoft local machine but not your personal Microsoft store (CAPI certificates). However, to use a CAPI certificate, you can log on using cached credentials, make a VPN connection using your CAPI certificate, and disable the "Disconnect VPN connection when logging off" parameter (see "Disconnecting When Logging Off of a Windows NT Platform," following). This action keeps your connection open. Now you can log back on to the system.

For information on enrolling certificates and importing certificates into your Cisco store, see "Enrolling and Managing Certificates."

For information about using start before logon with the Entrust SignOn feature, see "Connecting with an Entrust Certificate."

Turning Off Start Before Logon

To turn this feature off, open the Options pull-down menu on the VPN Dialer connection dialog box and uncheck **Enable start before logon**. The next time you log on to your system, the VPN Dialer connection dialog box does not automatically display on your logon desktop.

Permission to Launch an Application Before Log On

Your system administrator determines whether you can launch applications and third-party dialers before you log on to a Windows NT platform. To protect system and network security, your system administrator might have disabled this feature. If this feature is greyed out, you cannot launch applications and third-party dialers before logging on to a Windows NT platform. You must have system administrator privileges to change this parameter.

ECTI CPL AC
CPMI - CORREIOS
Fls. Nº 421
Doc. 3698

Disconnecting When Logging Off of a Windows NT Platform

This parameter controls whether your VPN Client connection automatically disconnects when you log off your Windows NT system.

To always automatically terminate your connection when you log off, check this parameter. This parameter is checked by default.

To disable auto-disconnect while logging off, remove the check from this parameter. When you remove the check, the VPN Client displays the warning message shown in Figure 5-19.

Figure 5-19 Auto-disconnect Warning Message

Disabling this parameter allows your connection to remain up during and after log off, which allows profiles or folders to be synchronized during log off. You would disable this parameter when using the Windows roaming profiles feature.

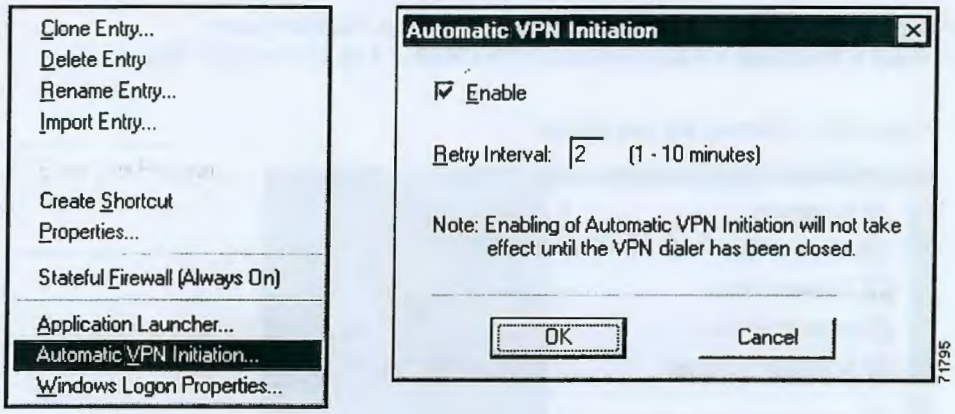
Note With this feature disabled, you must completely shut down your system to disconnect your VPN Client connection.

Managing Auto Initiation

When your network administrator has configured your VPN Client for auto initiation (by including it in the vpnclient.ini file), the Options menu includes the option Automatic VPN Initiation. (See Figure 5-20.) When you select this option, the VPN Dialer displays a dialog box that lets you enable/disable auto initiation and change the setting of the retry interval. Disabling auto initiation in this way does not remove it from your configuration. If you need to enable auto initiation after you have disabled it, you can return to this dialog box and enable it again. The only way you can remove auto initiation from your configuration is through editing the vpnclient.ini file.

For complete information on auto initiation, see "Using Automatic VPN Initiation".

Figure 5-20 Automatic VPN Initiation Option



To disable or enable auto initiation, follow these steps:

Step 1 Select **Automatic VPN Initiation** from the Options menu.

Step 2 To disable auto initiation, click to remove the check mark from **Enable**.

Or to enable auto initiation after it has been disabled, click **Enable** to check it.

Step 3 Click **OK**.

Step 4 If you are enabling auto initiation, you then must close the VPN Dialer. The authentication dialog then prompts you to enter your authentication information.

To change the setting of the retry interval, enter the new value (1 to 10) in the **Retry Interval** box and click **OK**.

Viewing and Managing the VPN Client Event Log

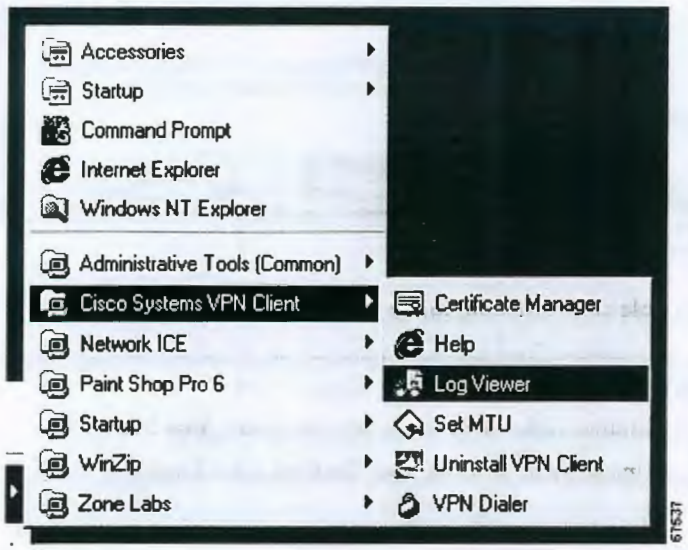
Examining the event log can often help a network administrator diagnose problems with an IPSec connection between a VPN Client and a peer device. The log viewer application collects event messages from all processes that contribute to the client-peer connection. This section shows how to use the Log Viewer to retrieve and manage this information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
422
Fls Nº
3698
Doc.

Starting the Log Viewer

To start the Log Viewer, use the following path from the Start menu:
Start > Programs > Cisco Systems VPN Client > Log Viewer. (See Figure 5-21.)

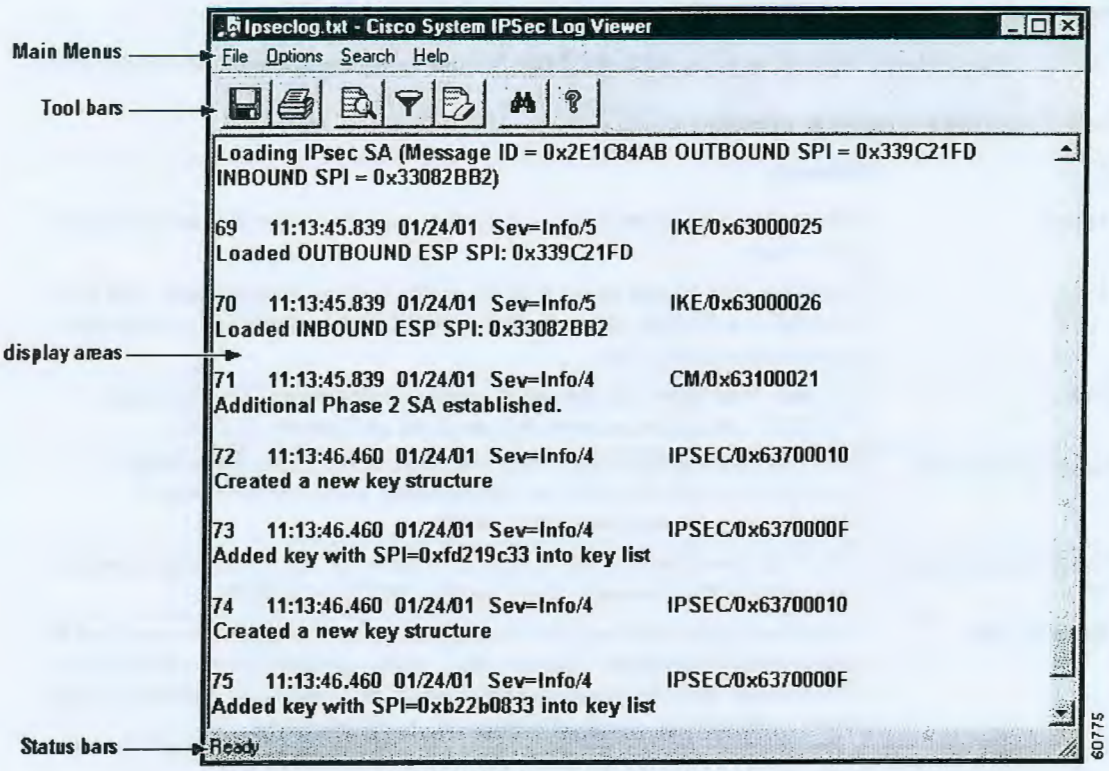
Figure 5-21 Starting the Log Viewer



The Log Viewer starts, displaying its main window. (See Figure 5-22.) By default, the filter is set to low, so you may not see any events displayed in this window (see the section "Filtering Events").

For help on this window, press **F1**.

Figure 5-22 Log Viewer Main Window



Displaying the Version of the Software

To display a brief help message that gives you the version number of the software, choose **Help** from the main menu or click the **Help** icon.

Collecting Events

To start collecting event messages into the log file, choose **Options > Capture**. When a check mark appears in front of the Capture option, Log Viewer is collecting events. This option is off by default. Alternatively, you can click the Capture icon.

RQS nº 03/2005
CPMI - CORREIOS
Fls Nº 423
3698
Doc.

Each message in the log file comprises at least two lines containing the following fields:

```
Event# Time Date Severity/type/level EventClass/MessageID
Message text
```

Table 5-1 describes the fields in an event message. Table 5-2 describes Event types and severity levels.

Table 5-1 Fields in an Event Message

Field	Meaning
Event#	The first field shows the event number. Events are numbered incrementally and never reset.
Time	The Time field shows the time of the event: *hour:minutes:seconds*. The hour is based on a 24-hour clock. For example 15:25:09 identifies an event that occurred at 3:25:09 PM.
Date	The date field shows the date of the event: *MM/DD/YYYY*. For example, 2/03/2001 identifies an event that occurred on February 3, 2001.
Severity/type/level	This field reports the severity type and level of the event; for example, Sev=Info/4, which identifies an informational event, severity level 4. identifies event types and severity levels
Event Class/Message ID	This field shows the module or source of the event and the message identifier associated with the module. For example, IPSEC/0x63700012.
Message Text	A brief message describing the event. Usually, this message is no more than 80 characters. For example, `Delete all keys associated with peer` 10.10.99.40. In a message containing arrows, the arrows indicate the direction of the transmission: >>> for sending and <<< for receiving.

Table 5-2 Event Types and Severity Levels

Type	Level	Meaning
Fault	1	A system failure or nonrecoverable error.
Warning	2 - 3	Imminent system failure or a serious problem that may require user intervention.
Informational	4 - 6	Level 4 provides the most general type (high level) information. Levels 5 and 6 provide more detailed information about the connection.

Filtering Events

To control the amount of information to view with the Log Viewer, choose **Options > Filter**. Alternatively, you can click the Filter icon.

The Log Viewer displays the Log Viewer Filter message to let you choose the amount of information you want to capture. (See Figure 5-23.)

Figure 5-23 Log Viewer Filter Message

To change the filter level, do the following:

Step 1 Double-click on one item, or choose more than one item and right click.

Step 2 Choose from the following options that the Log Viewer displays:

Disable—Inhibits event reporting for the chosen class.

Low—Provides the least amount of information. This choice includes severity levels 1 through 3 (all faults and warnings). Low is the default for all classes.

Medium—Includes severity levels 1 through 4; all in Low plus the first level informational events, which provide general information about the connection. Note that a first level informational event is level 4 and appears in the event display as Info/4.

High—Includes severity levels 1 through 6, thus adding two levels of informational events (Info/5 and Info/6). This setting can lower the performance of all applications on your system, so use it only when your network administrator or a support engineer suggests that you do so.

Table 5-3 defines the classes (modules) that generate events.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 424
Doc. 3698

Table 5-3 Classes That Generate Events in the VPN Client

Class Name	Definition
CERT	Certificate management process (CERT), which handles getting, validating, and renewing certificates from certificate authorities. CERT also displays errors that occur as you use the application.
CLI	Command Line Interface, which lets managers start and end connections, get status information and so on through a command line rather than using the VPN Client graphical user interface.
CM	Connection manager (CM), which drives VPN connections. (CM dials a PPP device, configures IKE for establishing secure connections, and manages connection states.
CVPND	Cisco VPN Daemon (main daemon), which initializes client service and controls messaging process and flow.
DIALER	Windows-only component, which handles configuring a profile, initiating a connection, and monitoring it.
FIREWALL	Firewall component, which generates events related to connections through a firewall.
IKE	Internet Key Exchange (IKE) module, which manages secure associations.
IPSEC	IPSec module, which obtains network traffic and applies IPSec rules to it.
PPP	Point-to-Point Protocol.
XAUTH	Extended authorization application, which validates a remote user's credentials.

Searching the Log File

To locate specific events or event types in the window, choose **Search** from the main menu. Alternatively, you can click on the Search icon.

The Log Viewer displays the **Find** message. (See Figure 5-24.) Enter a string to find and click **Find Next**. You can match on whole words and on case.

Figure 5-24 Searching the Log Display

Printing the Log File

To print the events displayed in the current window, choose **File > Print** from the main menu. Alternatively, you can click the Printer icon.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 425
Doc. 3698

Saving the Log File

To save the currently displayed events in the `ipseclog` file on your hard drive, choose **File > Save as** from the main menu. Alternatively, click the Disk icon.

The ipseclog file is a text (.txt) file in DOS format. The Log Viewer saves the information to the Client install directory, which by default is the pathname Program Files\Cisco Systems VPN Client\VPN Client\IPSECLOG.TXT. You can specify any directory and name. (See Figure 5-25.)

Figure 5-25 Saving a Log File

Clearing the Events Display

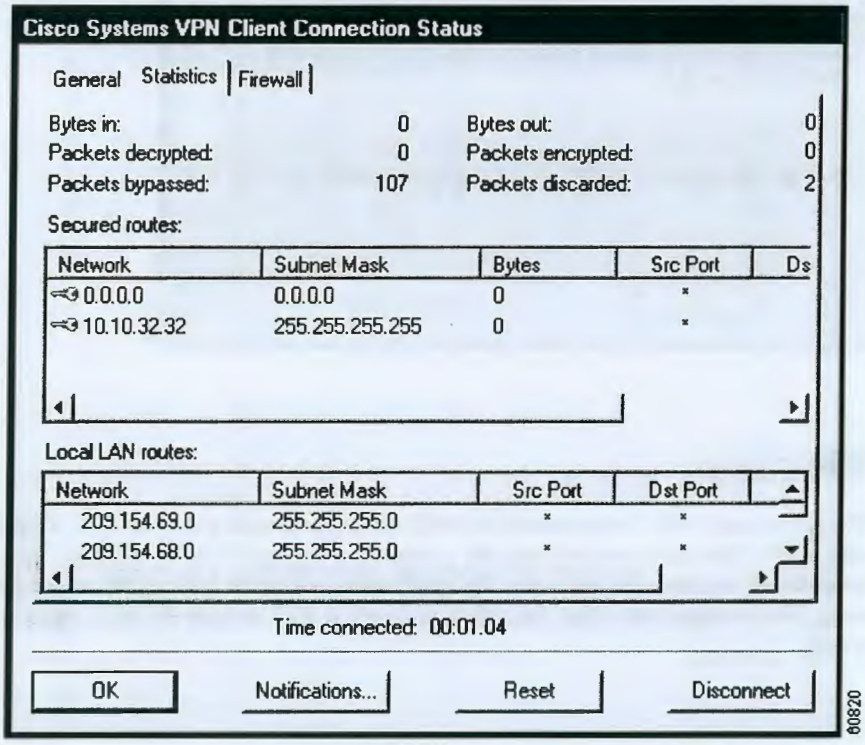
To eliminate all the events currently displayed in the Log Viewer main window, choose **Options > ClearLog Display** from the main menu. Alternatively, you can click the Erase All icon.

If you want to store the event messages, be sure you save them before you clear the display. Clearing the display does not reset event numbering, nor does it clear the log file itself.

Receiving Notifications From a VPN Device

The VPN device (secure gateway) through which you connect to the private network at your organization can send you notifications. Currently you can receive a notification from your network administrator when it is time to update the VPN Client software or when the VPN device that requires a specific firewall be running on the VPN Client PC detects that the firewall is not running. A notification typically shows up when you start your dialer connection. You can also display notifications while you are connected by clicking **Notifications** on the Connection Status dialog box. (See Figure 5-26.)

Figure 5-26 Displaying Notifications

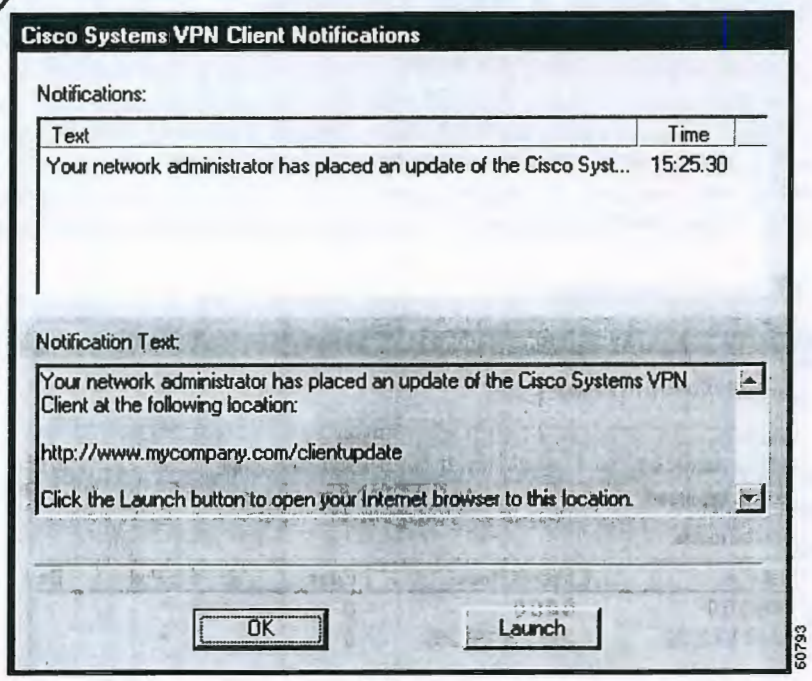


Upgrade Notifications

The notification shown in Figure 5-27 informs a remote user that it is time to upgrade the VPN Client software. The notification includes the location where the remote user can obtain the upgrade. When you receive an upgrade notification that includes a URL, click **Launch** to go to the site and retrieve the upgrade software. You will receive an upgrade notification every time you connect until you have installed the upgrade software.

CPMI - CORR
Fls. Nº 426
Doc. 3698

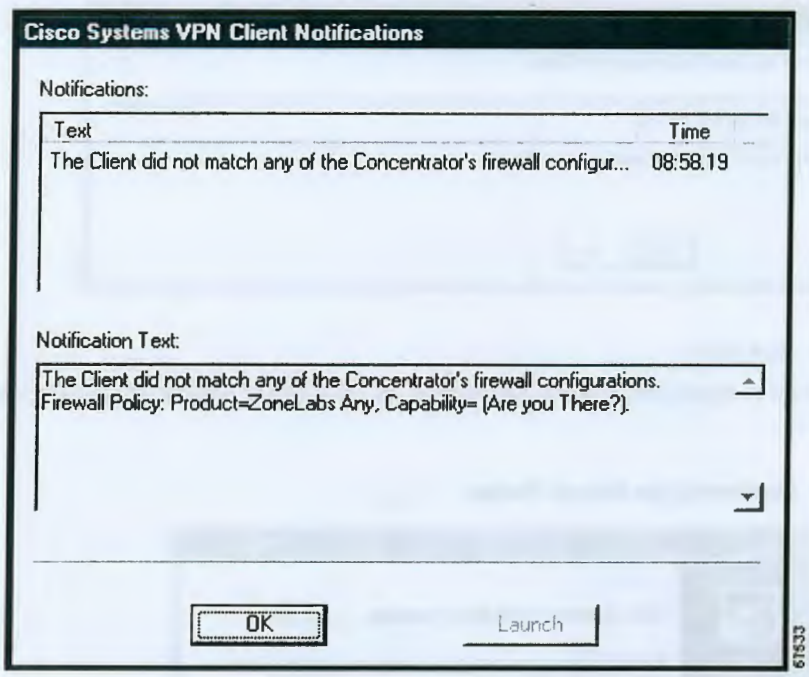
Figure 5-27 Notification of a Software Upgrade



Firewall Notifications

If the VPN Client and VPN Concentrator firewall configurations do not match, the VPN Concentrator notifies the VPN Client while negotiating the connection. The notification includes the policy that the VPN Concentrator requires. For example, the notification in Figure 5-28 shows an example firewall notification. The message states that the policy required is AYT and the firewall required is any Zone Labs product.

Figure 5-28 Firewall Notification



Upgrading the VPN Client Software (InstallShield)

Upgrading the VPN Client software using this method retains existing connection entries and their parameters.

To install an upgrade of the VPN Client over an existing version on your system, use the following procedure, which first uninstalls the existing version, and then reboots your PC and installs the new version.

Step 1 To begin the procedure, follow the instructions in the "Installing the VPN Client Through InstallShield" section in Chapter 2.

When it starts, the installation wizard detects the existing version and asks you to confirm that you want to remove that version and reboot your PC. (See Figure 5-29.)

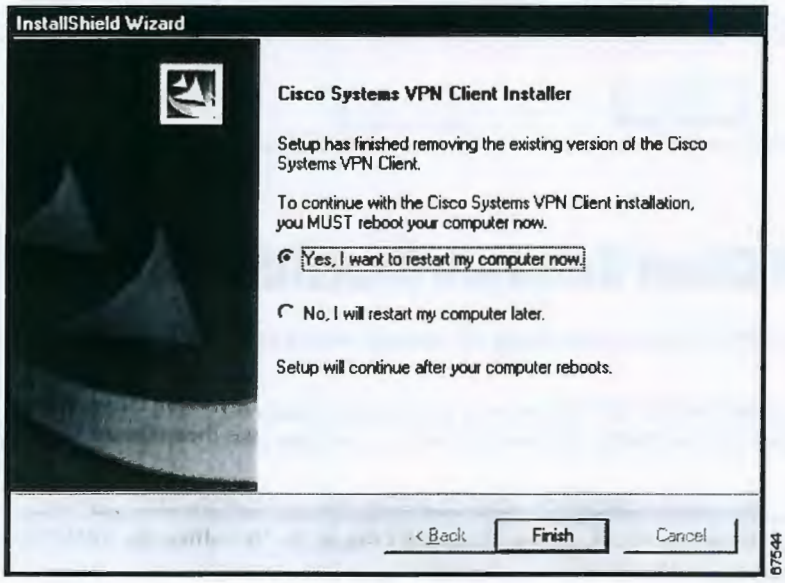
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 427
Doc. 3698

Figure 5-29 Uninstalling an Existing Version

Step 2 To continue, click **Yes**.

The installation program removes the old version and asks you to confirm the system restart. (See Figure 5-30.)

Figure 5-30 Confirming the System Restart



Be sure to remove any diskette from its drive before you restart your system.

If you are installing from diskettes, reinsert Disk 1 after your system restarts and displays the Windows logo screen, but *before* the desktop appears.

Step 3 To restart your system, click **Yes** (the default) and click **Finish**.

The installation wizard restarts your system. Once your system has restarted, installation continues automatically.

Step 4 Follow the instructions as if you were installing for the first time. See "Installing the VPN Client Through InstallShield."

Upgrading the VPN Client Software (MSI)

Upgrading the VPN Client software using this MSI in this recommended way retains existing connection entries and their parameters.

To install an upgrade of the VPN Client over an existing version on your system, use the following procedure.

Step 1 Remove any existing version of the VPN Client software through the Add/Remove available from the Windows Control Panel.

Step 2 Install the VPN Client using the MSI installer (vpnclient_en.msi).

Uninstalling the VPN Client with the Uninstall Application

This option is available only if you have installed the VPN Client via InstallShield. Uninstalling the VPN Client means completely removing all VPN Client software from your computer. For example, if you are changing or upgrading your PC, you might want to uninstall the VPN Client. Also, if you are getting ready to install Cisco VPN Client 3.6 using Microsoft Windows Installer (MSI), you can run the Uninstall application to remove previous versions of the Cisco VPN Client.

Note Do not attempt to uninstall or upgrade the VPN Client software from a mapped network drive.

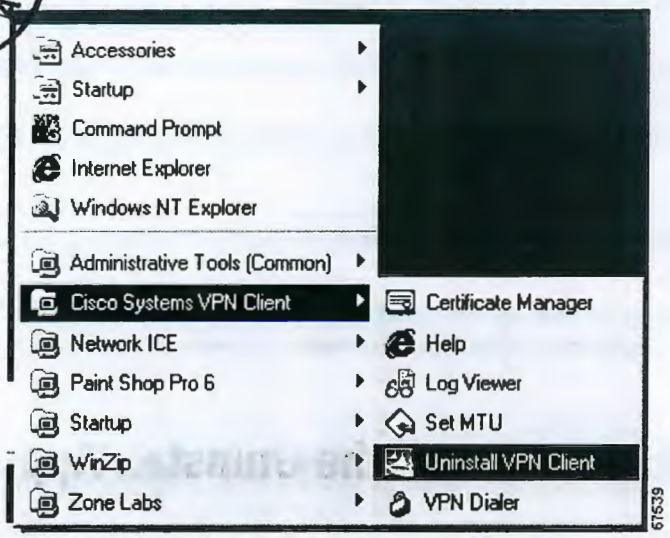
Before you run the uninstall program, make sure you have closed all of your remote access (Dial-Up Networking) connections and all VPN Client applications. Then use the following procedure. (See Figure 5-31.)

Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

Step 1 Choose **Start > Programs > Cisco Systems VPN Client > Uninstall VPN Client**.

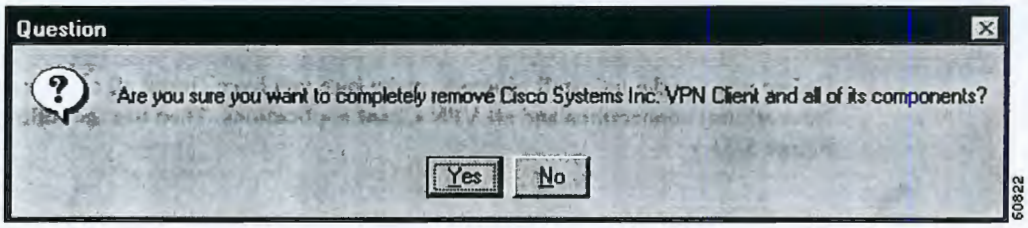
ECT 1466 21 CPL AC
IRQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 428
3698
Doc.

Figure 5-31 Running the Uninstall Program



The Uninstall Wizard runs and asks if you want to really want to remove the VPN Client applications. (See Figure 5-32.)

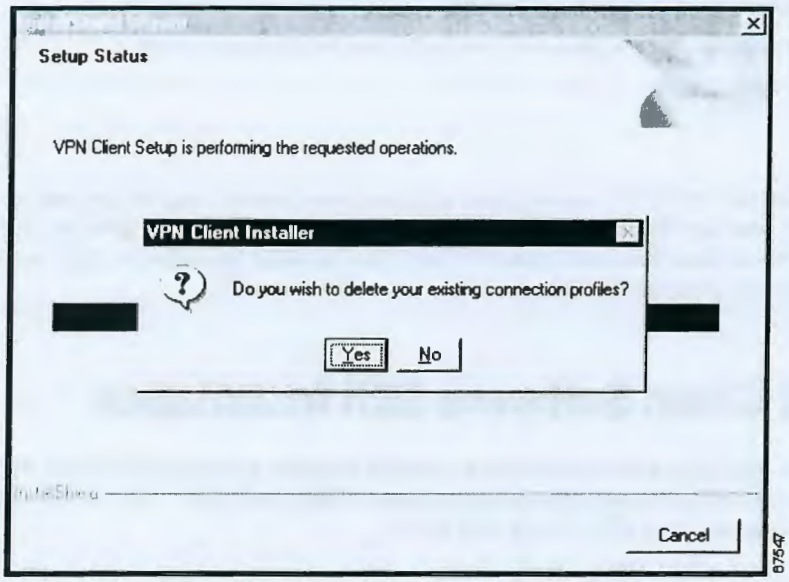
Figure 5-32 Confirming Uninstall



Step 2 To completely remove the VPN Client software from your system, click **Yes**. Otherwise, click **No**.

Next, the Uninstall Wizard asks if you want to delete your connection profiles. (See Figure 5-33.)

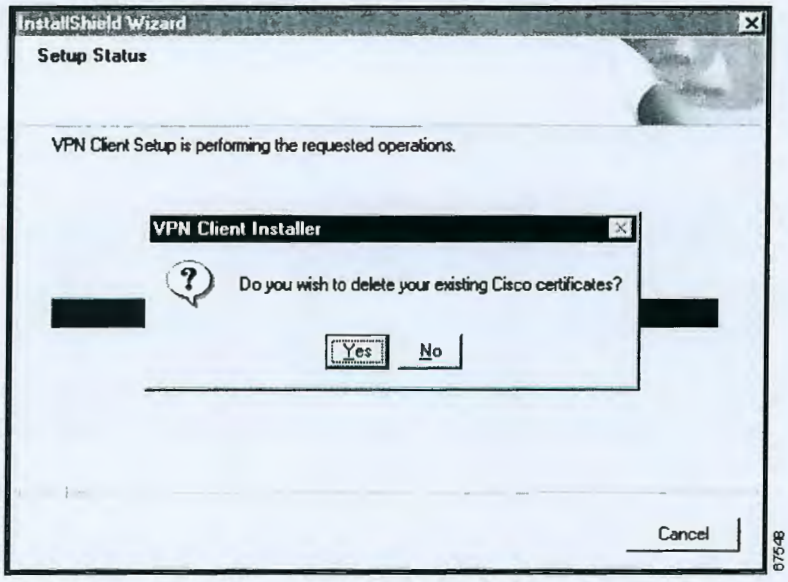
Figure 5-33 Confirming Your Connections



Step 3 To preserve your connection profiles (which contain configured connection entries), click **No**.

Then the Uninstall Wizard asks if you want to delete your certificates. (See Figure 5-34.)

Figure 5-34 Confirming Your Certificates



Step 4 To keep your certificates, click **No**.

Finally, the Uninstall Wizard prompts you to restart your system. To complete the uninstallation, you must restart your system.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 429
Doc: 3698

Step 5 To restart your system, click **Yes** (the default) and then click **Finish**.

The installation program restarts your system.

Be sure to remove any diskette from its drive before you restart your system.

Note When you uninstall the VPN Client software after you have run the Log Viewer and you have clicked yes to remove your certificate and profile directories, the vpnclient.ini and ipseclog.txt files remain on your system. Since these files were generated after you installed the software, they are not removed when you uninstall the software. You have to remove them manually.

Removing the VPN Client Software MSI Installation

To remove the VPN Client when it has been installed via MSI, use the Add/Remove utility available from the Control Panel. You must remove any version of the Cisco VPN Client or any other VPN Client before upgrading the Cisco VPN Client with MSI.

CHAPTER 6

Enrolling and Managing Certificates

This chapter explains how to enroll and manage personal certificates using the Certificate Manager application. Specifically, it describes how to perform the following tasks:

- Obtain personal certificates through enrollment with a Certificate Authority (CA), which is an organization that issues digital certificates that verify that you are who you say you are.

  You can enroll for a certificate in two ways:

  - through the network (*online enrollment)*
  - through a file
- Import certificates
- Manage certificates
  - Viewing
  - Verifying
  - Deleting
  - Exporting
- Manage enrollment requests

This chapter covers the following topics:

- Starting Certificate Manager
- What are Certificate Stores?
- Enrolling for a Certificate
- Managing Personal and CA/RA Certificates
- Managing Enrollment Requests

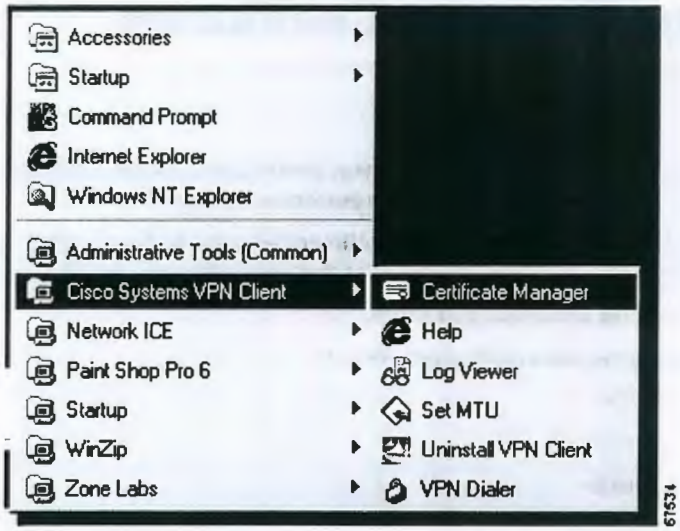
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 430
3698
Doc.

Starting Certificate Manager

To get started with certificates, go to the Cisco Systems VPN Client menu (the same menu that you use to start the client, shown in Figure 6-1).

Choose **Start> Programs> Cisco Systems VPN Client> Certificate Manager.**

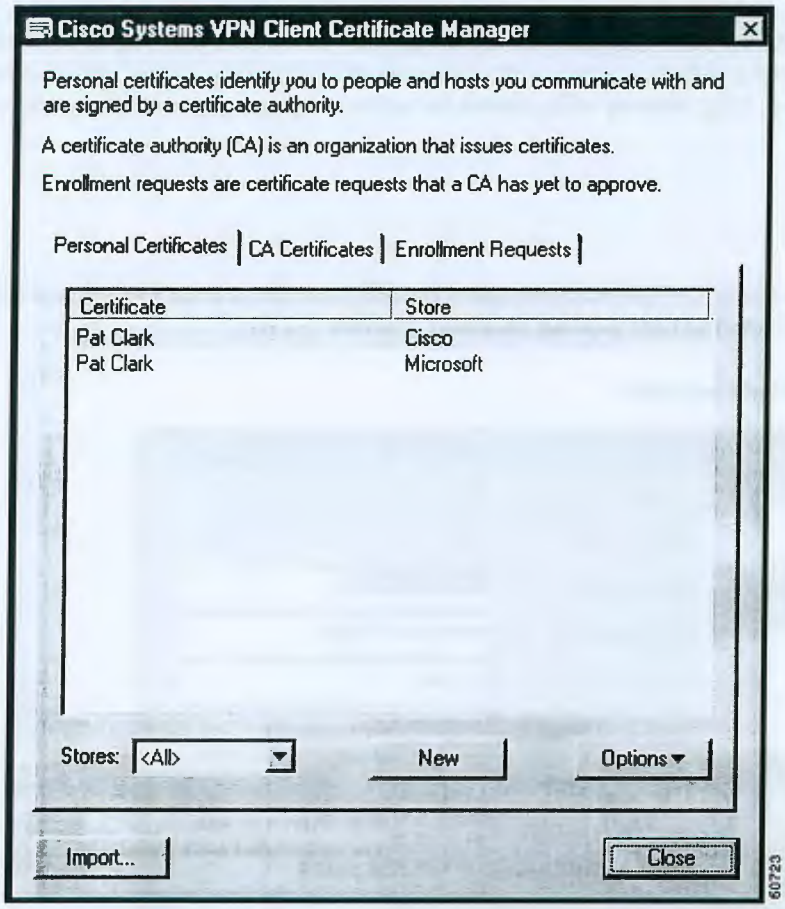
Figure 6-1 Choosing Certificate Manager



The Certificate Manager window opens. (See Figure 6-2.)

ECT 1068 CPL - AC

Figure 6-2 Certificate Manager Main Window



What are Certificate Stores?

The Certificate Manager uses the notion of *store* to convey a location in your local file system for storing personal certificates. The major store for the VPN Client is the Cisco store. The Cisco store contains certificates you have enrolled for through the Simple Certificate Enrollment Protocol (SCEP). This application supports several standard enrollment protocols. Your system also includes a Microsoft certificate store that may contain certificates that your organization provides or that you have installed previously. You can manage them just like the certificates in your Cisco store, or you can import them to your Cisco store. New certificates obtained through enrollment or importing go into the Cisco store.

There are two types of Microsoft certificates: certificates for individuals to use and also a Microsoft certificate for your local PC itself. So if several people are using the same PC, each person can have a certificate, and there can also be a certificate for the local system on Windows 2000 and Windows XP. On a Windows 9x system, you can only use it with Internet Explorer version 5.1 SP2.

Microsoft certificates with non-exportable private keys are also available.

POS nº 03/2005 - CN
CPMI - IOS
Fls. Nº 431
3698
Doc.

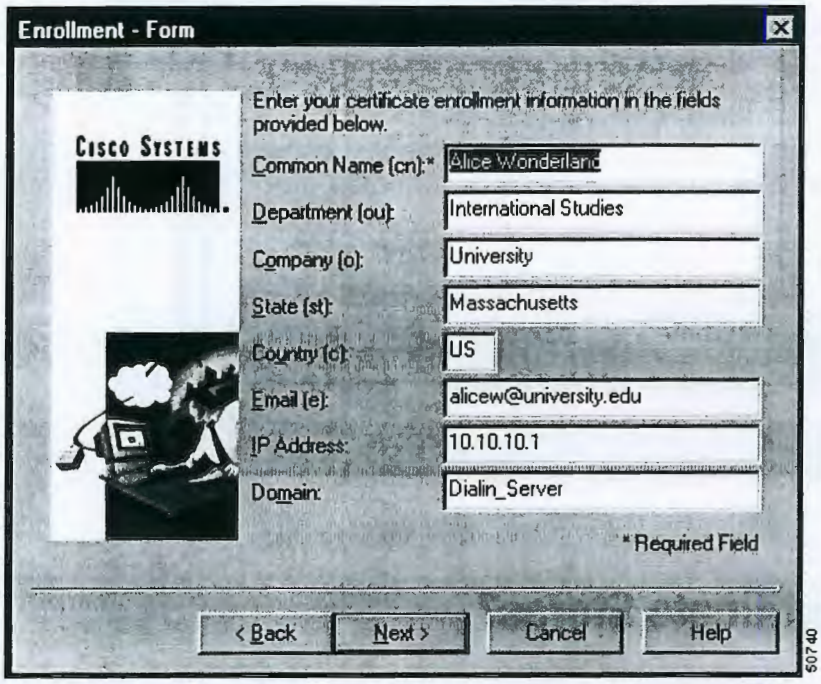
Enrolling for a Certificate

Your system administrator may have already set up your VPN Client with digital certificates. If not, or if you want to add certificates, you can obtain a certificate by enrolling with a Certificate Authority (CA) over the network or by creating a file request. In both cases, you complete the same form (shown in Figure 6-3.)

Enrollment Form

This section describes the information required for filling out the certificate enrollment form. Make sure you have all of the following information before you start.

Figure 6-3 Enrollment Form



- Common Name—Your common name (CN), which is the unique name to use for this certificate. This field is required. The common name can be the name of a person, system, or other entity; it is the most specific level in the identification hierarchy. The common name becomes the name of the certificate; for example, Alice Wonderland.
- Department—The name of the department to which you belong; for example, International Studies. This field correlates to the Organizational Unit (OU). The OU is the same as the Group Name configured in a VPN 3000 Series Concentrator, for example.
- Company—The name of the company or organization (O) to which you belong; for example, University.
- State—The name of your state (ST); for example, Massachusetts.

- Country—The 2-letter country code for your country (C); for example, US. This two-letter country code must conform to ISO 3166 country abbreviations.
- Email—Your email address (e); for example, alicew@university.edu.
- IP Address—The IP address of your system, for example, 10.10.10.1.
- Domain—The Fully Qualified Domain Name of the host for your system; for example, `Dialin_Server`.

Together, all these fields except IP address and domain comprise your distinguished name (DN).

When you enroll a personal certificate, either you go through a CA from which your system already has a root certificate or you obtain a root certificate from the CA as part of the enrollment process. The CA Certificates tab displays the current list of CA certificates. (See Figure 6-2.)

Starting Enrollment

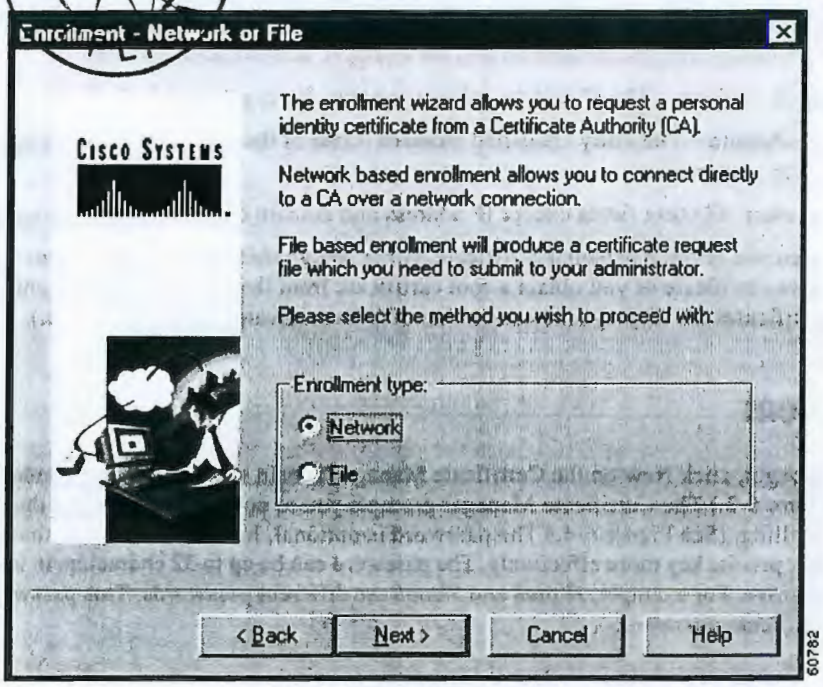
To begin, click **New** on the Certificate Manager's main screen under the Personal Certificates tab. (See Figure 6-2.) The Certificate Manager prompts you to enter a password for the certificate you are enrolling. (See Figure 6-4.) The password is optional, but we recommend that you use one to protect your private key more effectively. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords. This password is called the *personal certificate password*.

Figure 6-4 Protecting a Certificate with a Password

After entering a password, click **Next** to continue. The Certificate Manager lets you choose between enrolling via the network or by creating a file. (See Figure 6-5.) Enrolling via the network is also called *online enrollment*.

CPMI - CORREIOS
Fls. Nº 432
Doc. 3698

Figure 6-5 Choosing Enrollment Method



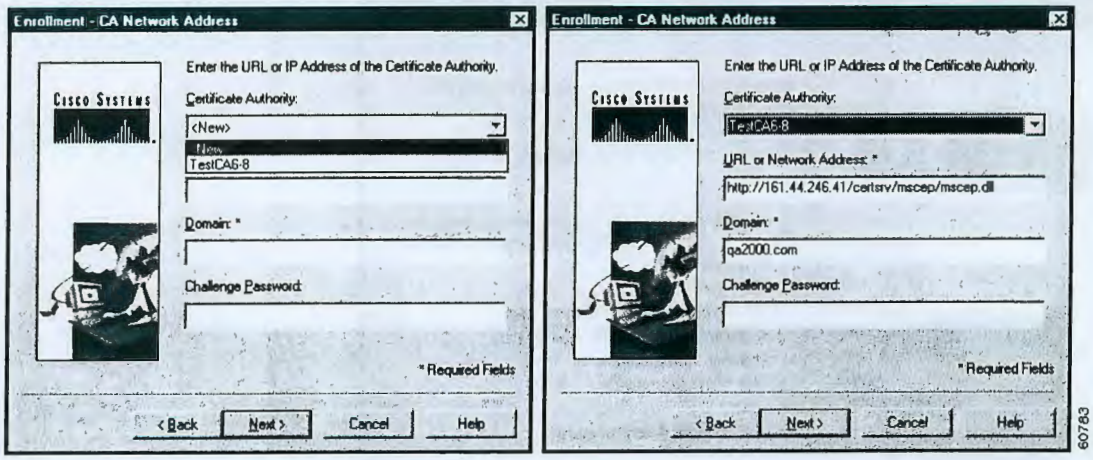
Enrolling Through the Network

To enroll through the network, retrieve a certificate from a CA, and place it in the Cisco store, using the following procedure:

Step 1 Click **Network** and click **Next**. (See Figure 6-5.)

The Certificate Manager asks you to enter the network address of the issuing CA. (See Figure 6-6.)

Figure 6-6 Entering Network Address



Step 2 Choose one of the following procedures:

- Choose an existing Certificate Authority from the drop-down menu.
  - The URL or Network Address and Domain fields are automatically filled.
  - Renter the Challenge password or enter a new password, which you can obtain from the CA or your network administrator.
- Choose **<New>** from the drop-down menu.
  - Enter the URL or Network Address of the CA and the CA's Domain, both of which are required.
  - Some CAs require that you enter a password to access their site. If this is the case, enter the password in the Challenge Password field. You can get the password from the CA or from your network administrator.

Step 3 When you have completed the network address information, click **Next**.

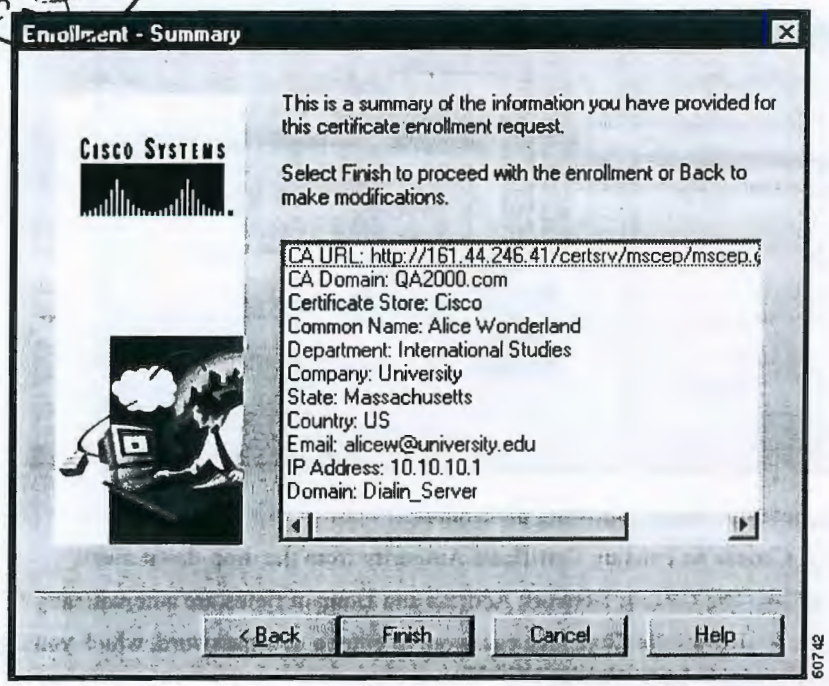
The Certificate Manager displays the enrollment form for you to complete. (See Figure 6-3.)

Step 4 Enter the information you collected before you started the enrollment process. The only field that the Certificate Manager requires is Common Name. However the CA may require some or all of the other fields. Then click **Next**.

After you enter the form, the Certificate Manager displays a summary that looks something like the one in Figure 6-7.

CPMI - CORREIOS
Fls. Nº 433
Doc. 3698

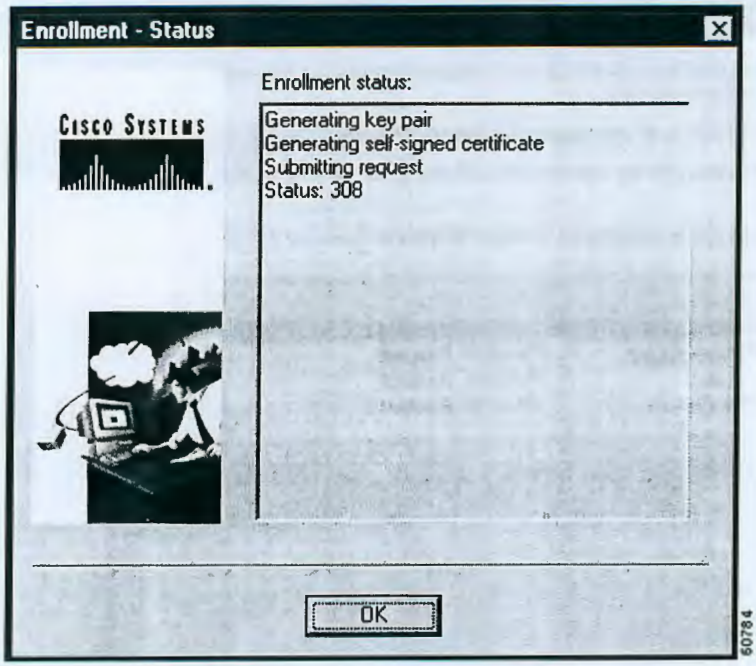
Figure 6-7 Enrollment Summary



Step 5 To complete the enrollment, click **Finish**.

The Certificate Manager displays a status window (shown in Figure 6-8) that lets you monitor the progress of the certificate retrieval. If the enrollment failed, the status window indicates the cause so you can fix the problem and try again.

Figure 6-8 Certificate Status Messages

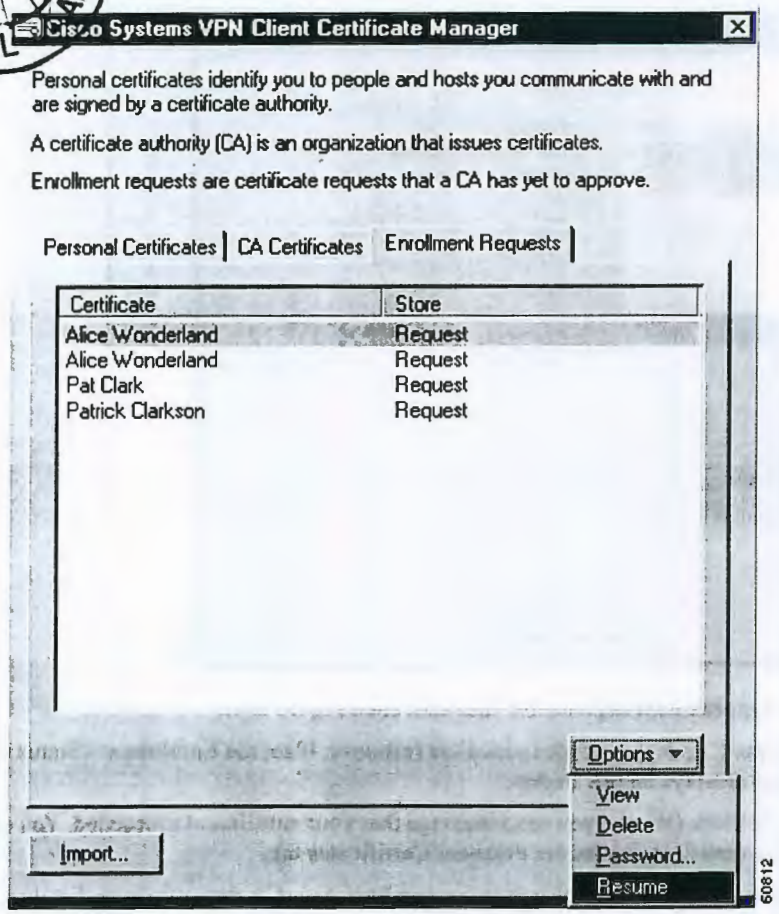


Step 6 What happens next depends on your CA. (See Figure 6-8):

- Some CAs may provide immediate response. If so, the Enrollment - Status window reflects this fact and displays an OK button.
  - Click **OK** and you see a message that your enrollment succeeded. You can view and manage the certificate under the Personal Certificates tab.
- If the enrollment status is Request pending, your CA does not immediately approve your request and the Enrollment - Status window shows the Suspend button.
  - Click **Suspend**.
  - Your request appears under the Enrollment Requests tab, while you are waiting for the CA to issue the certificate.
  - When the CA issues your certificate, choose the certificate and then choose **Resume** from the Options pull-down menu to complete the enrollment. (See Figure 6-9.)

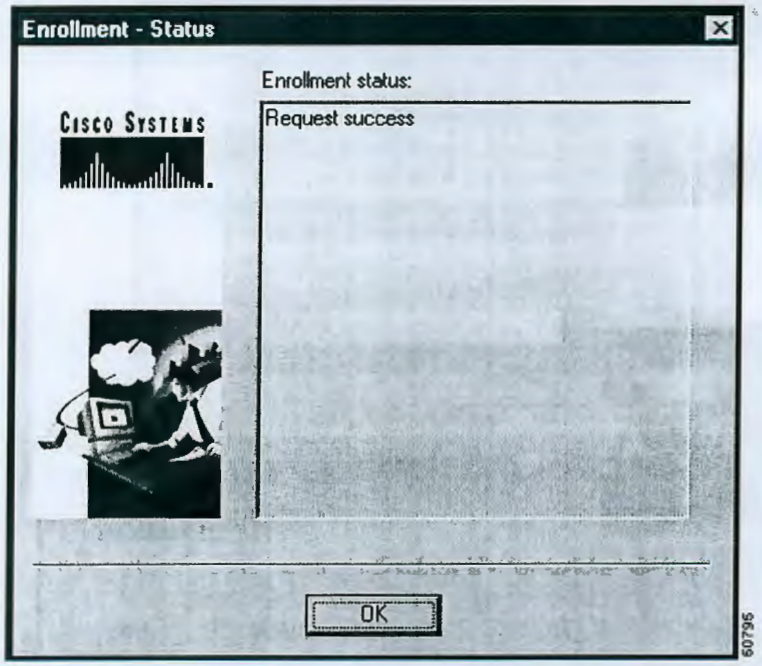
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 434
Doc. 3698

Figure 6-9 Resuming Enrollment Request



- After you have obtained the certificate, the status screen updates to show the result. (See Figure 6-10.) After viewing the screen, click **OK**.

Figure 6-10 Receiving Status Update



Enrolling Through a File Request

Alternatively, you can enroll by creating a file using the same form as network enrollment. (See Figure 6-3.) Once you have created a request file, you can either e-mail it to the CA and receive a certificate back or you can access the CA's website and cut and paste the enrollment request in the area that the CA provides.

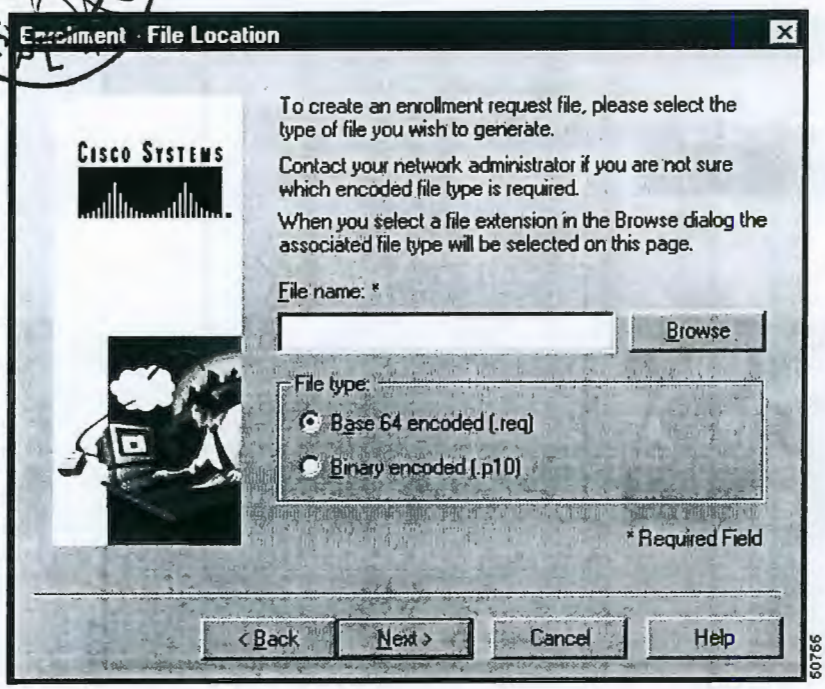
To enroll through a file request, use the following procedure:

Step 1 At the Enrollment - Network or File dialog box. (See Figure 6-5), click **File** and click **Next**.

The Certificate Manager prompts you to choose a file type for your file request and to specify a file name. (See Figure 6-11.)

ECTI CPL AC
BOS nº 03/2005 - CN
CPMI - 6-11 EIOS
Fls. Nº 435
Doc. 3698

Figure 6-11 Choosing file type and location



Step 2 Click one of the following file types:

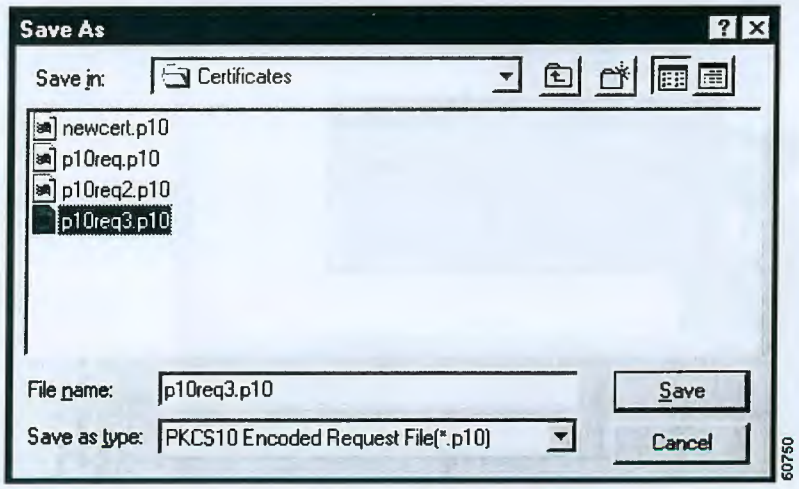
- **Binary encoded**—A base-2 PKCS10 file (Public Key Cryptography Standard; for example, an X.509 DER file). You cannot display a binary-encoded file.
- **Base 64 encoded**—An ASCII-encoded PKCS10 file that you can display in text format (for example, the request shown in Figure 6-12). Choose this type when you want to cut and paste the text into the CA website.

Figure 6-12 A PKCS10 Certificate Request

Step 3 Enter the full pathname for the file request.

When you browse for an appropriate directory for placing the file request, the Certificate Manager shows only the files of the chosen file type. (See Figure 6-13.) You can save your file enrollment requests in the Certificates directory, which is a subdirectory of the directory where the VPN Client is installed.

Figure 6-13 Specifying a Filename

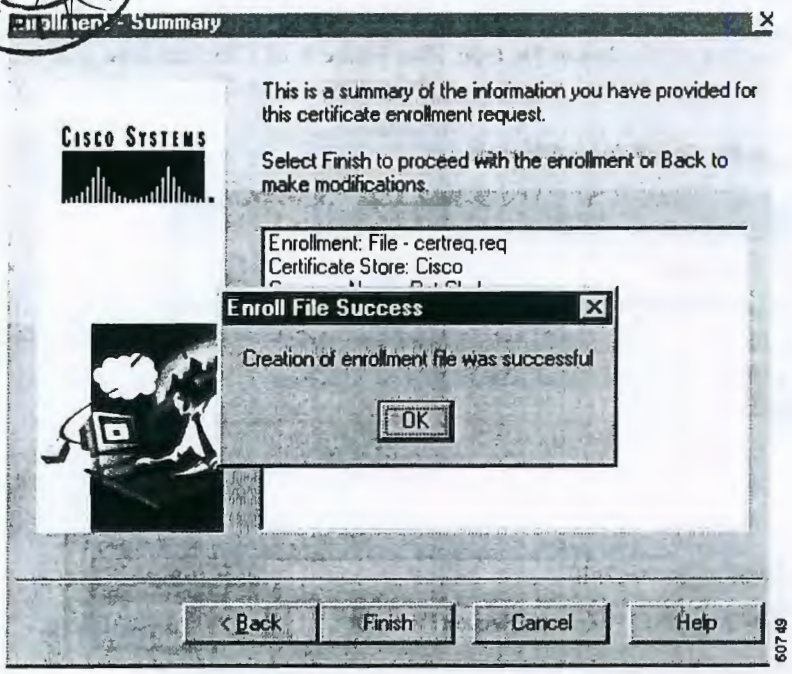


In this example, the complete pathname is C:\Program Files\Cisco Systems\VPN Client\Certificates\p10req3.p10.

Step 4 Complete the form (see the "Enrollment Form" section) and click **Next**.

The Certificate Manager displays the summary screen and a message to let you know that your request succeeded. (See Figure 6-14.)

Figure 6-14 Enroll File Success Message



Step 5 Click **OK** on the message screen then click **Finish** on the summary screen.

You can view the file request under the Enrollment Requests tab. (See Figure 6-15.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 437
Doc. 3698

CHAPTER 6

User Group Management

This chapter provides information about setting up and managing user groups in Cisco Secure Access Control Server (Cisco Secure ACS) Appliance version 3.2 to control authorization. Cisco Secure ACS enables you to group network users for more efficient administration. Each user can belong to only one group in Cisco Secure ACS. You can establish up to 500 groups to effect different levels of authorization.

Cisco Secure ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, these groups can be mapped into Cisco Secure ACS. And if the external database does not support groups, you can map all users from that database to a Cisco Secure ACS user group. For information about external database mapping, see Chapter 15, "User Group Mapping and Specification".

Before you configure Group Setup, you should understand how this section functions. Cisco Secure ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by settings in the Network Configuration and Interface Configuration sections.

This chapter contains the following sections:

- **User Group Setup Features and Functions, page 6-2**—This section is an overview of the features you find within Group Setup.
- **Common User Group Settings, page 6-3**—This section details procedures that you typically would perform regardless of your particular network security configuration.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 438
Doc. 3698

- Configuration-specific User Group Settings, page 6-15—This section details procedures that you would perform only as applicable to your particular network security configuration.
- Group Setting Management, page 6-52—This section includes basic administrative procedures, such as determining the users in a group or renaming a group.

User Group Setup Features and Functions

The Group Setup section of the Cisco Secure ACS HTML interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see Network Device Group Configuration, page 4-36.

Default Group

If you have not configured group mapping for an external user database, Cisco Secure ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, Cisco Secure ACS retains the group mappings you configured before upgrading.

Group TACACS+ Settings

Cisco Secure ACS enables a full range of settings for TACACS+ at the group level. If a AAA client has been configured to use TACACS+ as the security control protocol, you can configure standard service protocols, including PPP IP, PPP LCP, ARAP, SLIP, and shell (exec), to be applied for the authorization of each user who belongs to a particular group.

Note You can also configure TACACS+ settings at the user level. User-level settings always override group level settings.

Cisco Secure ACS also enables you to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see Protocol Configuration Options for TACACS+, page 3-7.

If you have configured Cisco Secure ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about Cisco Secure ACS interaction with device-management applications, see Support for Cisco Device-Management Applications, page 1-18.

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. This feature enables you to apply shell commands to a particular user group in the following ways:

- Assign a shell command authorization set, which you have already configured, for any network device.
- Assign a shell command authorization set, which you have already configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command authorization sets, see Chapter 5, "Shared Profile Components".

Common User Group Settings

This section presents the basic activities you perform when configuring a new user group. This section contains the following procedures:

- Enabling VoIP Support for a User Group, page 6-4
- Setting Default Time-of-Day Access for a User Group, page 6-5
- Setting Callback Options for a User Group, page 6-6
- Setting Network Access Restrictions for a User Group, page 6-7
- Setting Max Sessions for a User Group, page 6-11
- Setting Usage Quotas for a User Group, page 6-13

RQS nº 0[redacted]6-3
CPMI - CORREIOS
Fls. Nº 439
Doc. 3698

Enabling VoIP Support for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Group Settings** check box.

Perform this procedure to enable support for the null password function of VoIP. This enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users do not need to enter passwords to authenticate.

Caution Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes.

To enable VoIP support for a group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group you want to configure for VoIP support, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Voice-over-IP Support table, select the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.

Step 4 To save the group settings you have just made, click **Submit**.
For more information, see Saving Changes to User Group Settings, page 6-54.

Step 5 To continue, and specify other group settings, perform other procedures in this chapter, as applicable.

Setting Default Time-of-Day Access for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Default Time-of-Day / Day-of-Week Specification** check box.

To define the times during which users in a particular group are permitted or denied access, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Default Time-of-Day Access Settings table, select the **Set as default Access Times** check box.

Note You must select the **Set as default Access Times** check box to limit access based on time or day.

Result: Times at which the system permits access are highlighted in green on the day and hour matrix.

Note The default sets accessibility during all hours.

Step 4 In the day and hour matrix, click the times at which you do *not* want to permit access to members of this group.

Tip Clicking times of day on the graph deselects those times; clicking again reselects them.
At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

RQS 65 - CN
CPMI - CORREIOS
Fls. Nº 440
Doc. 3698

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Callback Options for a User Group

Callback is a command string that is passed back to the access server. You can use callback strings to initiate a modem to call the user back on a specific number for added security or reversal of line charges. There are three options, as follows:

- **No callback allowed**—Disables callback for users in this group. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.
- **Use Windows Database callback settings (where possible)**—Uses the Microsoft Windows callback settings. If a Windows account for a user resides in a remote domain, the domain in which Cisco Secure ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.

To set callback options for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 Select a group from the Group list, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Callback table, select one of the following three options:

- No callback allowed
- Dialup client specifies callback number
- Use Windows Database callback settings (where possible)

Step 4 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Network Access Restrictions for a User Group

The Network Access Restrictions table in Group Setup enables you to apply network access restrictions (NARs) in three distinct ways:

- Apply existing shared NARs by name.
- Define IP-based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS-based group NARs to permit or deny access to either, or both, the calling line ID (CLI) number or the Dialed Number Identification Service (DNIS) number used.

Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see About Network Access Restrictions, page 5-7.

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can be applied to more than one group or user. For more information, see Shared Network Access Restrictions Configuration, page 5-9. You must have enabled the Group-Level Shared Network Access Restriction check box on the Advanced Options page of the Interface Configuration section for these options to appear in the Cisco Secure ACS HTML interface.

However, Cisco Secure ACS also enables you to define and apply a NAR for a single group from within the Group Setup section. You must have enabled the Group-Level Network Access Restriction setting under the Advanced Options page of the Interface Configuration section for single group IP-based filter options and single group CLI/DNIS-based filter options to appear in the Cisco Secure ACS HTML interface.

RQS nº 6-7
CPMI - CORREIOS
441
Fls. Nº
3698
Doc.

Note When an authentication request is forwarded by proxy to a Cisco Secure ACS server, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 To apply a previously configured shared NAR to this group, follow these steps:

Note To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see Shared Network Access Restrictions Configuration, page 5-9.

a. Select the **Only Allow network access when** check box.

b. To specify whether one or all shared NARs must apply for a member of the group to be permitted access, select one of the following options:

- All selected shared NARS result in permit
- Any one selected shared NAR results in permit

c. Select a shared NAR name in the Shared NAR list, and then click —> (right arrow button) to move the name into the Selected Shared NARs list.

Tip To view the server details of the shared NARs you have selected to apply, you can click either **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Step 4 To define and apply a NAR, for this particular user group, that permits or denies access to this group based on IP address, or IP address and port, follow these steps:

Tip You should define most NARs from within the Shared Components section so that the restrictions can be applied to more than one group or user. For more information, see Shared Network Access Restrictions Configuration, page 5-9.

a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, select the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select either **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.

c. Select or enter the information in the following boxes:

- **AAA Client**—Select either All AAA Clients or the name of the NDG or the name of the individual AAA client to which to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to filter on when performing access restrictions. You can use the wildcard asterisk (*).

Note The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

d. Click **Enter**.

Result: The specified the AAA client, port, and address information appears in the NAR Access Control list.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 442
3698
Doc.

Step 5 To permit or deny access to this user group based on calling location or values other than an established IP address, follow these steps:

a. Select the **Define CLI/DNIS-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one of the following:

- Permitted Calling/Point of Access Locations
- Denied Calling/Point of Access Locations

c. From the AAA Client list, select either All AAA Clients or the name of the NDG or the name of the particular AAA client to which to permit or deny access.

d. Complete the following boxes:

Note You must type an entry in each box. You can use the wildcard asterisk (*) for all or part of a value. The format you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **PORT**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

Tip This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet client MAC address. For more information, see About Network Access Restrictions, page 5-7.

- **DNIS**—Type the DNIS number to restrict access based on the number into which the user will be dialing. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

Tip This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet AP MAC address. For more information, see About Network Access Restrictions, page 5-7.

Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

e. Click **Enter**.

Result: The information, specifying the AAA client, port, CLI, and DNIS appears in the list.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Max Sessions for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Max Sessions** check box.

Perform this procedure to define the maximum number of sessions available to a group, or to each user in a group, or both. The settings are as follows:

- **Sessions available to group**—Sets the maximum number of simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.

Tip As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than 5 users can log in.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 443
3698
Doc.

Note A session is any type of connection supported by RADIUS or TACACS+, such as PPP, NAS prompt, Telnet, ARAP, IPX/SLIP.

Note The default setting for group Max Sessions is Unlimited for both the group and the user within the group.

To configure max sessions settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Max Sessions table, under Sessions available to group, select one of the following options:

- **Unlimited**—Select to allow this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow this group.

Step 4 In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:

- **Unlimited**—Select to allow each individual in this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow each user in this group.

Note Settings made in User Setup override group settings. For more information, see Setting Max Sessions Options for a User, page 7-16.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Usage Quotas for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Usage Quotas** check box.

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- By total duration of session
- By the total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users assigned to that group, unless you configure usage quotas for the individual users.

Note The Usage Quotas section on the Group Settings page does not show usage statistics.
Usage statistics are available only on the settings page for an individual user. For more information, see Setting User Usage Quotas Options, page 7-18.

When a user exceeds his or her assigned quota, Cisco Secure ACS denies that user access upon attempting to start a session. If a quota is exceeded during a session, Cisco Secure ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see Resetting Usage Quota Counters for a User Group, page 6-53.

Tip To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated when the user logs off. If the AAA client through which the user is accessing your

RQS nº 03/2005 - CN
CPMI - CORREIOS
444
Fls. Nº
3698
Doc.

network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate. This means that a second channel will be accepted even if the first channel has exhausted the quota for the user.

To set user usage quotas for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 To define usage quotas based on duration of sessions, follow these steps:

a. In the Usage Quotas table, select the **Limit each user of this group to** *x* **hours of online time** *per time unit* check box.

b. Type the number of hours to which you want to limit group members in the **to** *x* **hours** box.
Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.

Note Up to 5 characters are allowed in the to *x* hours box.

c. Select the period for which the quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of hours, with no end.

Step 4 To define user session quotas based on number of sessions, follow these steps:

a. In the Usage Quotas table, select the **Limit each user of this group to** *x* **sessions** check box.

b. Type the number of sessions to which you want to limit users in the **to *x* sessions** box.

Note Up to 5 characters are allowed in the to *x* sessions box.

c. Select the period for which the session quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of session, with no end.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

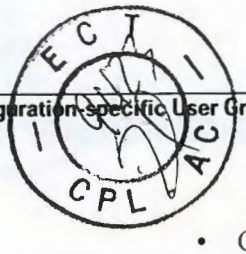
Configuration-specific User Group Settings

This section details procedures that you perform only as applicable to your particular network security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.

This section contains the following procedures:

- Setting Token Card Settings for a User Group, page 6-17
- Setting Enable Privilege Options for a User Group, page 6-18
- Enabling Password Aging for the CiscoSecure User Database, page 6-20
- Enabling Password Aging for Users in Windows Databases, page 6-25
- Setting IP Address Assignment Method for a User Group, page 6-27
- Assigning a Downloadable IP ACL to a Group, page 6-28
- Configuring TACACS+ Settings for a User Group, page 6-29

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 445
Doc



- Configuring a Shell Command Authorization Set for a User Group, page 6-31
- Configuring a PIX Command Authorization Set for a User Group, page 6-33
- Configuring Device-Management Command Authorization for a User Group, page 6-35
- Configuring IETF RADIUS Settings for a User Group, page 6-37
- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-38
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-39
- Configuring Ascend RADIUS Settings for a User Group, page 6-41
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-42
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-44
- Configuring Microsoft RADIUS Settings for a User Group, page 6-45
- Configuring Nortel RADIUS Settings for a User Group, page 6-47
- Configuring Juniper RADIUS Settings for a User Group, page 6-49
- Configuring BBSM RADIUS Settings for a User Group, page 6-50

Note When a vendor-specific variety of RADIUS is configured for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, used as the first 74 attributes for all RADIUS vendors.

The content of these subsections is dynamic and based on two factors as follows:

- For a particular protocol to be listed, a AAA client must be configured to authenticate using that protocol. For more information, see AAA Client Configuration, page 4-11.
- The specific attributes for a particular protocol must be configured for display at the group level. For more information, see Protocol Configuration Options for TACACS+, page 3-7 or Protocol Configuration Options for RADIUS, page 3-11.

Setting Token Card Settings for a User Group

Note If this section does not appear, configure a token server. Then, click **External User Databases**, click **Database Configuration**, and then add the applicable token card server.

Perform this procedure to allow a token to be cached. This means users can use a second B channel without having to enter a second one-time password (OTP).

Caution This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select both Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Token Cards**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 446
Doc. 3691

Step 4 In the Token Card Settings table, to cache the token for the entire session, select **Session**.

Step 5 Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication), follow these steps:

a. Select **Duration**.

b. Type the duration length in the box.

c. Select the unit of measure, either Seconds, Minutes or Hours.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Enable Privilege Options for a User Group

Note If this section does not appear, click **Interface Configuration** and then click **TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, select the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enable parameters. The three possible TACACS+ enable options are as follows:

- **No Enable Privilege**—(default) Select this option to disallow enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Select this option to select the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Select this option to define maximum privilege levels for an NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.

Note To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, click **Interface Configuration**, click **Advanced Settings**, and then select the **Network Device Groups** check box.

If you are using NDGs, this option lets you configure the NDG for enable-level mapping rather than having to do it for each user in the group.

To set enable privilege options for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Enable Options**.

Step 4 Do one of the following:

- To disallow enable privileges for this user group, select the **No Enable Privilege** option.
- To set the maximum privilege level for this user group, for any ACS on which this group is authorized, select the **Max Privilege for Any Access Server** option. Then, select the maximum privilege level from the list.
- To define the maximum NDG privilege level for this user group, select the **Define max Privilege on a per-network device group basis** option. Then, from the lists, select the NDG and a corresponding privilege level. Finally, click **Add Association**.

  Result: The association of NDG and maximum privilege level appears in the table.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 447
Doc. 3698

Enabling Password Aging for the CiscoSecure User Database

The password aging feature of Cisco Secure ACS enables you to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules)
- After a specified number of logins (age-by-uses rules)
- The first time a new user logs in (password change rule)

Varieties of Password Aging Supported by Cisco Secure ACS

Cisco Secure ACS supports four distinct password aging mechanisms, as follows:

- **EAP-GTC Windows Password Aging**—Users must be in the Windows user database and be using a Microsoft client that supports EAP, such as Windows XP. For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-25.
- **RADIUS-based Windows Password Aging**—Users must be in the Windows user database and be using the Windows Dial-up Networking (DUN) client. For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-25.
- **Password Aging for Device-hosted Sessions**—Users must be in the CiscoSecure user database, the AAA client must be running TACACS+, and the connection must use Telnet. You can control the ability of users to change passwords during a device-hosted Telnet session. You can also control whether Cisco Secure ACS propagates passwords changed by this feature. For more information, see Local Password Management, page 8-5.
- **Password Aging for Transit Sessions**—Users must be in the CiscoSecure user database. Users must use a PPP dialup client. Further, the end-user client must have CiscoSecure Authentication Agent (CAA) installed.

Tip The CAA software is available at http://www.cisco.com.

Also, to run password aging for transit sessions, the AAA client can be running either RADIUS or TACACS+; and the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of

the calling station. (Watchdog packets are interim packets sent periodically during a session. They provide an approximate session length in the event that no stop packet is received to mark the end of the session.)

You can control whether Cisco Secure ACS propagates passwords changed by this feature. For more information, see Local Password Management, page 8-5.

Cisco Secure ACS supports password aging using the RADIUS protocol under MS CHAP versions 1 and 2. Cisco Secure ACS does not support password aging over Telnet connections using the RADIUS protocol.

Caution If a user with a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the change password option does not appear, and the user account is expired.

Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows Password Aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-25. For information on configuring local password validation options, see Local Password Management, page 8-5.

The password aging feature in Cisco Secure ACS has the following options:

- **Apply age-by-date rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by date. The age-by-date rules contain the following settings:
  - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
  - **Warning period**—The number of days users will be notified to change their passwords. The existing password can be used, but the Cisco Secure ACS presents a warning indicating that the password must be changed and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 448
Doc. 1698

- **Grace period**—The number of days to provide as the user grace period. The grace period allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be disabled if the password is not changed, and enables the user to change it. Continuing with the examples above, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. Cisco Secure ACS displays the "last chance" warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.

Note All passwords expire at midnight, not the time at which they were set.

- **Apply age-by-uses rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
  - **Issue warning after *x* logins**—The number of the login upon which Cisco Secure ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

  - **Require change after *x* logins**—The number of the login after which to notify users that they must to change their passwords. Continuing with the previous example, if this number is set to 12, users receive prompts requesting them to change their passwords on their 11th and 12th login attempts. On the 13th login attempt, they receive a prompt telling them

that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the **Issue warning after *x* login** number.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Selecting this check box forces new users to change their passwords the first time they log in.
- **Generate greetings for successful logins**—Selecting this check box enables a Greetings message to display whenever users log in successfully via the CAA client. The message contains up-to-date password information specific to this user account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are checked, passwords never expire.

Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts expire and appear in the Accounts Disabled list.

Before You Begin

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, either TACACS+ RADIUS.
- Verify that you have configured your password validation options. For more information, see Local Password Management, page 8-5.
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of the calling station.

RQS nº 03/2005 - CN
CPMI - CORREIOS
449
Fls. Nº
3698
Doc.

To set password aging rules for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Password Aging**.

Result: The Password Aging Rules table appears.

Step 4 To set password aging by date, select the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:

- Active period
- Warning period
- Grace period

Note Up to 5 characters are allowed in each field.

Step 5 To set password aging by use, select the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:

- Issue warning after *x* logins
- Require change after *x* logins

Note UP to 5 characters are allowed in each field.

Step 6 To force the user to change the password on the first login after an administrator has changed it, select the **Apply password change rule** check box.

Step 7 To enable a Greetings message display, select the **Generate greetings for successful logins** check box.

Step 8 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 9 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Enabling Password Aging for Users in Windows Databases

Cisco Secure ACS supports two types of password aging for users in Windows databases. Both types of Windows password aging mechanisms are separate and distinct from the other Cisco Secure ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the CiscoSecure user database, see Enabling Password Aging for the CiscoSecure User Database, page 6-20.

Note You can run both Windows Password Aging and Cisco Secure ACS Password Aging for Transit Sessions mechanisms concurrently, provided that the users authenticate from the two different databases.

The two types of password aging in Windows databases are as follows:

- **RADIUS-based password aging**—RADIUS-based password aging depends upon the RADIUS AAA protocol to send and receive the password change messages. Requirements for implementing the RADIUS-based Windows password aging mechanism include the following:
  - Communication between Cisco Secure ACS and the AAA client must be using RADIUS.
  - The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
  - Users must be in a Windows user database.
  - Users must be using the Windows DUN client.
  - You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows configuration within the External User Databases section.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 450
Doc. 3698

Tip For information on enabling MS CHAP for password changes, see Configuring Windows Authentication, page 13-22. For information on enabling MS CHAP in System Configuration, see Global Authentication Setup, page 10-11.

- **PEAP password aging**—PEAP password aging depends upon the PEAP(EAP-GTC) or PEAP(EAP-MSCHAPv2) authentication protocol to send and receive the password change messages. Requirements for implementing the PEAP Windows password aging mechanism include the following:
  - The AAA client must support EAP.
  - Users must be in a Windows user database.
  - Users must be using a Microsoft PEAP client, such as Windows XP.
  - You must enable PEAP on the Global Authentication Configuration page within the System Configuration section.

Tip For information about enabling PEAP in System Configuration, see Global Authentication Setup, page 10-11.

  - You must enable PEAP password changes on the Windows Authentication Configuration page within the External User Databases section.

Tip For information about enabling PEAP password changes, see Configuring Windows Authentication, page 13-22.

Users whose Windows accounts reside in "remote" domains (that is, not the domain within which Cisco Secure ACS is running) can only use the Windows-based password aging if they supply their domain names.

The methods and functionality of Windows password aging differ according to which Microsoft Windows operating system you are using, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows user database is only one part of the

larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows system documentation.

Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way Cisco Secure ACS assigns IP addresses to users in the group. The four possible methods are as follows:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client network settings for TCP/IP.
- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool assigned on the AAA server.

To set an IP address assignment method for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **IP Address Assignment**.

Step 4 In the IP Assignment table, do one of the following:

- Select **No IP address assignment**.
- Select **Assigned by dialup client**.
- Select **Assigned from AAA Client pool**. Then, type the AAA client IP pool name.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 451
Doc: 3698

- Select **Assigned from AAA pool**. Then, select the AAA server IP pool name in the Available Pools list and click —> (right arrow button) to move the name into the Selected Pools list.

Note If there is more than one pool in the Selected Pools list, the users in this group are assigned to the first available pool in the order listed.

Tip To change the position of a pool in the list, select the pool name and click **Up** or **Down** until the pool is in the position you want.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Assigning a Downloadable IP ACL to a Group

The Downloadable ACLs feature enables you to assign an IP ACL at the group level.

Note You must have established one or more IP ACLs before attempting to assign one. For instructions on how to add a downloadable IP ACL using the Shared Profile Components section of the Cisco Secure ACS HTML interface, see Adding a Downloadable IP ACL, page 5-4.

Tip The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration**, click **Advanced Options**, and then select the **Group-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Downloadable ACLs**.

Step 4 Under the Downloadable ACLs section, click the **Assign IP ACL** check box.

Step 5 Select an IP ACL from the list.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring TACACS+ Settings for a User Group

Perform this procedure to configure and enable the service/protocol parameters to be applied for the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see Configuring a Shell Command Authorization Set for a User Group, page 6-31.

Note To display or hide additional services or protocols, click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select or clear items in the group column, as applicable.

To configure TACACS+ settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 452
Doc. 3698

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 To configure services and protocols in the TACACS+ Settings table to be authorized for the group, follow these steps:

a. Select one or more service/protocol check boxes (for example, PPP IP or ARAP).

b. Under each service/protocol that you selected in Step a, select attributes and then type in the corresponding values, as applicable, to further define authorization for that service/protocol.

To employ custom attributes for a particular service, you must select the **Custom attributes** check box under that service, and then specify the attribute/value in the box below the check box.

For more information about attributes, see Appendix B, "TACACS+ Attribute-Value Pairs", or your AAA client documentation.

Tip For ACLs and IP address pools, the name of the ACL or pool as defined on the AAA client should be entered. (An ACL is a list of Cisco IOS commands used to restrict access to or from other devices and users on the network.)

Note Leave the attribute value box blank if the default (as defined on the AAA client) should be used.

Note You can define and download an ACL. Click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select **Display a window for each service selected in which you can enter customized TACACS+ attributes**. A box opens under each service/protocol in which you can define an ACL.

Step 5 To allow all services to be permitted unless specifically listed and disabled, you can select the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.

Caution This is an advanced feature and should only be used by administrators who understand the security implications.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User Group

Use this procedure to specify the shell command authorization set parameters for a group. There are four options:

- **None**—No authorization for shell commands.
- **Assign a Shell Command Authorization Set for any network device**—One shell command authorization set is assigned, and it applies to all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Enables you to associate particular shell command authorization sets to be effective on particular NDGs.
- **Per Group Command Authorization**—Enables you to permit or deny specific Cisco IOS commands and arguments at the group level.

Note This feature requires that you have previously configured a shell command authorization set. For detailed steps, see Command Authorization Sets Configuration, page 5-19.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 153
3698
Doc.

To specify shell command authorization set parameters for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scrollbar to scroll to the Shell Command Authorization Set feature area.

Step 5 To prevent the application of any shell command authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular shell command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command authorization set you want applied to this group.

Step 7 To create associations that assign a particular shell command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and a corresponding **Command Set**.

Tip You can select a **Command Set** that will be effective for all **Device Groups**, that are not otherwise assigned, by assigning that set to the *<default>* Device Group.

c. Click **Add Association**.

Result: The associated NDG and shell command authorization set appear in the table.

Step 8 To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level, follow these steps:

a. Select the **Per Group Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select either **Permit** or **Deny**.

If you select Permit, users can issue all commands not specifically listed. If you select Deny, users can issue only those commands listed.

c. To list particular commands to be permitted or denied, select the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments should be permitted or denied.

Caution This is a powerful, advanced feature and should be used by an administrator skilled with Cisco IOS commands. Correct syntax is the responsibility of the administrator. For information on how Cisco Secure ACS uses pattern matching in command arguments, see About Pattern Matching, page 5-19.

Tip To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box you just completed.

Configuring a PIX Command Authorization Set for a User Group

Use this procedure to specify the PIX command authorization set parameters for a user group. There are three options:

- **None**—No authorization for PIX commands.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command authorization set is assigned, and it applies all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command authorization sets are to be effective on particular NDGs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
FTS. Nº 454
Doc 3698

Before You Begin

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- On the TACACS+ (Cisco) page of Interface Configuration section, ensure that the PIX Shell (pixShell) option is selected in the Group column.
- Make sure that you have already configured one or more PIX command authorization sets. For detailed steps, see Command Authorization Sets Configuration, page 5-19.

To specify PIX command authorization set parameters for a user group,

---

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.

Step 5 To prevent the application of any PIX command authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular PIX command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command authorization set you want applied to this user group.

Step 7 To create associations that assign a particular PIX command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

Result: The associated NDG and PIX command authorization set appear in the table.

Note To remove or edit an existing PIX command authorization set association, you can select the association from the list, and then click **Remove Association**.

Configuring Device-Management Command Authorization for a User Group

Use this procedure to specify the device-management command authorization set parameters for a group. Device-management command authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use Cisco Secure ACS for authorization. There are three options:

- **None**—No authorization is performed for commands issued in the applicable Cisco device-management application.
- **Assign a** *device-management application* for any network device—For the applicable device-management application, one command authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a** *device-management application* on a per Network Device Group Basis—For the applicable device-management application, this option enables you to apply command authorization sets to specific NDGs, so that it affects all management tasks on the network devices belonging to the NDG.

Note This feature requires that you have configured a command authorization set for the applicable Cisco device-management application. For detailed steps, see Command Authorization Sets Configuration, page 5-19.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 455
3698
Doc.

To specify device-management application command authorization for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scrollbar to scroll to the *device-management application* feature area, where *device-management application* is the name of the applicable Cisco device-management application.

Step 5 To prevent the application of any command authorization set for the applicable device-management application, select the **None** option.

Step 6 To assign a particular command authorization set that affects device-management application actions on any network device, follow these steps:

a. Select the **Assign a** *device-management application* for any network device option.

b. Then, from the list directly below that option, select the command authorization set you want applied to this group.

Step 7 To create associations that assign a particular command authorization set that affects device-management application actions on a particular NDG, for each association, follow these steps:

a. Select the **Assign a** *device-management application* on a per Network Device Group Basis option.

b. Select a **Device Group** and a corresponding **device-management application**.

c. Click **Add Association**.

Result: The associated NDG and command authorization set appear in the table.

Configuring IETF RADIUS Settings for a User Group

These parameters appear only when both the following are true:

- A AAA client has been configured to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes have been enabled on the RADIUS (IETF) page in the Interface Configuration section of the HTML interface.

RADIUS attributes are sent as a profile for each user from Cisco Secure ACS to the requesting AAA client. To display or hide any of these attributes, see Protocol Configuration Options for RADIUS, page 3-11. For a list and explanation of RADIUS attributes, see Appendix C, "RADIUS Attributes". For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.

To configure IETF RADIUS attribute settings to be applied as an authorization for each user in the current group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **RADIUS (IETF)**.

Step 4 For each IETF RADIUS attribute you need to authorize for the current group, select the check box next to the attribute and then define the authorization for the attribute in the field or fields next to it.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor supported by Cisco Secure ACS, see the appropriate section:

- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-38
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-39
- Configuring Ascend RADIUS Settings for a User Group, page 6-41
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-42

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 456
Doc. 3698

- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-44
- Configuring Microsoft RADIUS Settings for a User Group, page 6-45
- Configuring Nortel RADIUS Settings for a User Group, page 6-47
- Configuring Juniper RADIUS Settings for a User Group, page 6-49
- Configuring BBSM RADIUS Settings for a User Group, page 6-50

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco IOS/PIX RADIUS Settings for a User Group

The Cisco IOS/PIX RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX) attributes have been enabled in Interface Configuration: RADIUS (Cisco IOS/PIX).

Cisco IOS/PIX RADIUS represents only the Cisco VSAs. You must configure both the IETF RADIUS and Cisco IOS/PIX RADIUS attributes.

Note To hide or display Cisco IOS/PIX RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco IOS/PIX RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Before you configure Cisco IOS/PIX RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 For the Cisco attributes, determine the attributes to be authorized for the group by selecting the check box next to the attribute, and then type the commands (such as TACACS+ commands) to be packed as a RADIUS VSA.

Step 3 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 4 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco Aironet RADIUS Settings for a User Group

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. It acts as a specialized implementation (that is, a remapping) of the IETF RADIUS Session-Timeout attribute (27) to respond to a request from a Cisco Aironet Access Point. You use it to provide a different timeout values when users in a group must be able to connect via both wireless and wired devices. This capability to provide a second timeout value specifically for WLAN connections avoids the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes). You do not need to use Cisco-Aironet-Session-Timeout if all members of a group will always connect only with a Cisco Aironet Access Point. Rather, use this setting when a group may connect via wired or wireless clients.

For example, imagine a user group's Cisco-Aironet-Session-Timeout set to 600 seconds (10 minutes) and that same user group's IETF RADIUS Session-Timeout set to 3 hours. When a member of this group connects via a VPN, Cisco Secure ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet Access Point, Cisco Secure ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS Session-Timeout attribute. Thus, with the

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 457
3698
Doc.

Cisco-Aironet-Session-Timeout attribute configured, different session timeout values can be sent depending on whether the end-user client is a wired device or a Cisco Aironet Access Point.

The Cisco-Aironet-Session-Timeout VSA appears on the Group Setup page only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco Aironet) in Network Configuration.
- The group-level RADIUS (Cisco Aironet) attribute has been enabled in Interface Configuration: RADIUS (Cisco Aironet).

Note To hide or display the Cisco Aironet RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco Aironet)**.

Step 5 In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.

Step 6 In the [5842\001] Cisco-Aironet-Session-Timeout box, type the session timeout value (in seconds) that Cisco Secure ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS Session-Timeout attribute, see Appendix C, "RADIUS Attributes" or your AAA client documentation.

Step 7 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 8 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes have been enabled in Interface Configuration: RADIUS (Ascend).

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure both the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting displayed for RADIUS is `Ascend-Remote-Addr`.

Note To hide or display Ascend RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 458
3698
Doc.

To configure and enable Ascend RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.

Step 5 In the Ascend RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Be sure to define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes" or your AAA client documentation.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco

VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Cisco VPN 3000 Concentrator RADIUS attribute configurations appear only if both the following are true:

- A AAA client has been configured to use RADIUS (Cisco VPN 3000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000) attributes have been enabled on the RADIUS (Cisco VPN 3000) page of the Interface Configuration section.

Cisco VPN 3000 Concentrator RADIUS represents only the Cisco VPN 3000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 3000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 3000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 3000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000)**.

Step 5 In the Cisco VPN 3000 Concentrator RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Further define the authorization for that attribute in the field next to it.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 459
Doc. 3698

For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations display only when both the following are true:

- A network device has been configured to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes have been enabled on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.

Step 5 In the Cisco VPN 5000 Concentrator RADIUS Attributes table, select the attributes that should be authorized for the group by selecting the check box next to the attribute. Further define the authorization for each attribute in the field next to it.

For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

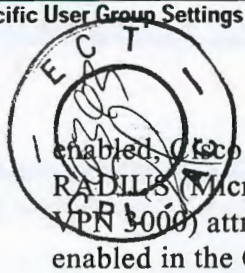
Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs supporting MPPE, which is an encryption technology developed by Microsoft to encrypt PPP links. These PPP connections can be via a dial-in line, or over a VPN tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 460
Doc. 3698



enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- Group-level Microsoft RADIUS attributes have been enabled on the RADIUS (Microsoft) page of the Interface Configuration section.

The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX
- Cisco VPN 3000
- Ascend

Microsoft RADIUS represents only the Microsoft VSA. You must configure both the IETF RADIUS and Microsoft RADIUS attributes.

Note To hide or display Microsoft RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Microsoft RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.

Step 5 In the Microsoft RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes have been enabled on the RADIUS (Nortel) page of the Interface Configuration section.

Nortel RADIUS represents only the Nortel VSA. You must configure both the IETF RADIUS and Nortel RADIUS attributes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 461
Doc. 3698

Note To hide or display Nortel RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Nortel RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.

Step 5 In the Nortel RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Juniper RADIUS Settings for a User Group

Juniper RADIUS represents only the Juniper VSA. You must configure both the IETF RADIUS and Juniper RADIUS attributes.

Note To hide or display Juniper RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Juniper RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

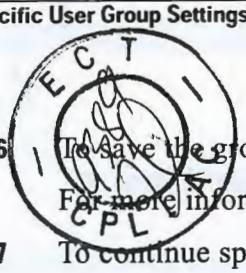
Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.

Step 5 In the Juniper RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 462
Doc. 3698



Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring BBSM RADIUS Settings for a User Group

BBSM RADIUS represents only the BBSM RADIUS VSA. You must configure both the IETF RADIUS and BBSM RADIUS attributes.

Note To hide or display BBSM RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable BBSM RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (BBSM)**.

Step 5 In the BBSM RADIUS Attributes table, specify the attribute to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-26.)
- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- Group-level custom RADIUS attributes have been enabled on the RADIUS (*Name*) page of the Interface Configuration section.

You must configure both the IETF RADIUS and the custom RADIUS attributes.

To configure and enable custom RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (*custom name*)**.

Step 5 In the RADIUS (*custom name*) Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Group Setting Management

This section describes how to use the Group Setup section to perform a variety of managerial tasks.

This section contains the following procedures:

- Listing Users in a User Group, page 6-53
- Resetting Usage Quota Counters for a User Group, page 6-53
- Renaming a User Group, page 6-54
- Saving Changes to User Group Settings, page 6-54

Listing Users in a User Group

To list all users in a specified group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 Click **Users in Group**.

Result: The User List page for the particular group selected opens in the display area.

Step 4 To open a user account (to view, modify, or delete a user), click the name of the user in the User List.

Result: The User Setup page for the particular user account selected appears.

Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, either before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 In the Usage Quotas section, select the **On submit reset all usage counters for all users of this group** check box.

Step 4 Click **Submit** at the bottom of the browser page.

Result: The usage quota counters for all users in the group are reset. The Group Setup Select page appears.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 464
Doc. 3698

Renaming a User Group

To rename a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 Click **Rename Group**.

Result: The Renaming Group: *Group Name* page appears.

Step 4 Type the new name in the **Group** field. Group names cannot contain angle brackets (< or >).

Step 5 Click **Submit**.

Note The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value associated with the group.

Result: The Select page opens with the new group name selected.

Saving Changes to User Group Settings

After you have completed configuration for a group, be sure to save your work.

To save the configuration for the current group, follow these steps:

Step 1 To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, and then click **Service Control**, and click **Restart**.

Tip To save your changes and apply them immediately, click **Submit + Restart**.

Result: The group attributes are applied and services are restarted. The Edit page opens.

Note Restarting the service clears the Logged-in User Report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.

Step 2 To verify that your changes were applied, select the group and click **Edit Settings**. View the settings.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 465
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 466
Doc. 3698

Cisco Systems

Data Sheet

CiscoWorks **Campus Manager**

Campus Manager is a key component in the CiscoWorks family of management solutions designed to make Cisco networks the most manageable and available in the industry. Today's networks are critical business assets, and require sophisticated tools for administering, monitoring and configuring Layer 2 services. Designed for enterprise network operations staff, Campus Manager provides powerful tools with built-in network intelligence to reduce the complexity and automate manual tasks associated with maintaining complex physical and logical network infrastructures.

Campus Manager Overview

Campus networks are at the heart of business and mission-critical systems. The requirement to understand, monitor, and react to changing networking conditions drives the need for sophisticated, yet easy-to-use management tools. Campus Manager is part of the LAN Management Solution, part of the broad range of CiscoWorks network management solutions.

New in Version 3.3:

In addition to the rich set of management features already included, the new version of Campus Manager has been enhanced to provide even greater manageability for Cisco networks. New benefits include:

- Improved application performance
- Doubled capacity for tracking end users

Key Campus Manager features include:

- Intelligent discovery and display of Layer 2 networks on browser-accessible topology maps, independent of VTP server
- Configuration of virtual LAN (VLAN)/ LAN Emulation (LANE) and asynchronous transfer mode (ATM) services and assignment of switch ports to those services
- Link and device status display based upon Simple Network Management Protocol (SNMP) polling
- Identification of Layer 2 configuration discrepancies
- Diagnostic tools for connectivity related problems between end stations, and Layer 2 and Layer 3 devices
- Automatic location and correlation of information on users by media access control (MAC), IP address, NT or NetWare Directory Services (NDS) login or UNIX host name, with their physical connections to the switched network
- Visibility and launch point of Cisco CallManager from topology services as well as tracking of phone handset to IP, Mac address, and switch port
- Layer 2 and Layer 3 path trace between source and destination handsets
- Export of topology maps to Visio
- Java plugins to improve graphical user interface (GUI) performance

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 467
Doc. 3698

- Ability to form Custom Groups in Topology View based on criteria like SysLocation, SysName and IP address/ Subnet mask.
- Secure communication between the client browser and Campus applications using Secure Socket Layer (SSL) protocol.

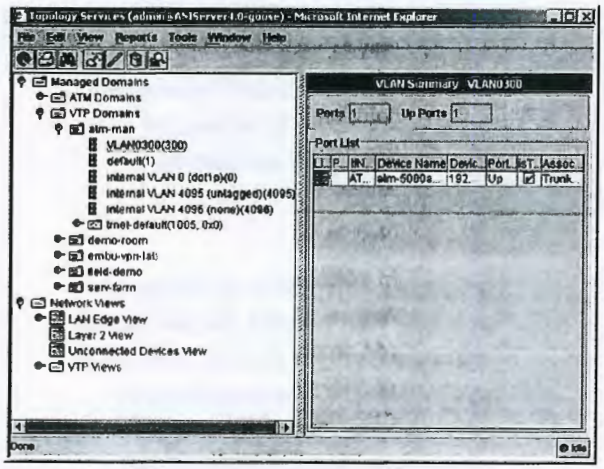
Campus Manager enables administrators to more easily change, monitor, and control network relationships, making them more effective in delivering business-critical and advanced networking services to their users and customers.

Campus Manager is a suite of applications launched from a common "management desktop" used by all Web-based CiscoWorks applications. Campus Manager contains three applications that can be launched from the client's browser:

- Topology Services—This is the principal interface to a variety of large scale topology maps, tabular summaries, reports, and configuration services of the Layer 2 network. A directory-like tree interface lists physical Layer 2 and logical, Virtual Trunking Protocol (VTP), and ATM domain views along with table summaries of the devices and interface associated with these views. This tree structure acts as the launching point for topology maps, discrepancy reporting functions, and configuration services. The integrated VLAN and LANE configuration capabilities, ATM soft permanent virtual circuit (PVC) configuration and diagnostic tools, along with physical and logical configuration discrepancy checking reports and highlighting tools are found within the Topology Services menus. It also supports discovery and display of Cisco Customer Response Applications, and reports on services of these devices.

  Ability to form custom groups based on dynamic and static rules for the group membership. System defined groups and user defined grouping can be created by network administrators and users respectively and allows grouping by developing rules based on criteria such as IP address, subnets, SysLocation, SysName, SysContact, Image Version and hostname. A rules editor allows for creating, editing Topology groups and defines rules for membership.

Figure 1
Topology Services Tabular View



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 2
VTP Domain Topology Map

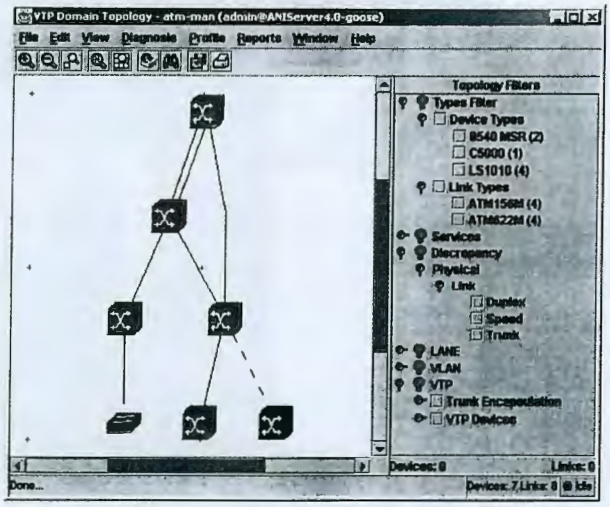
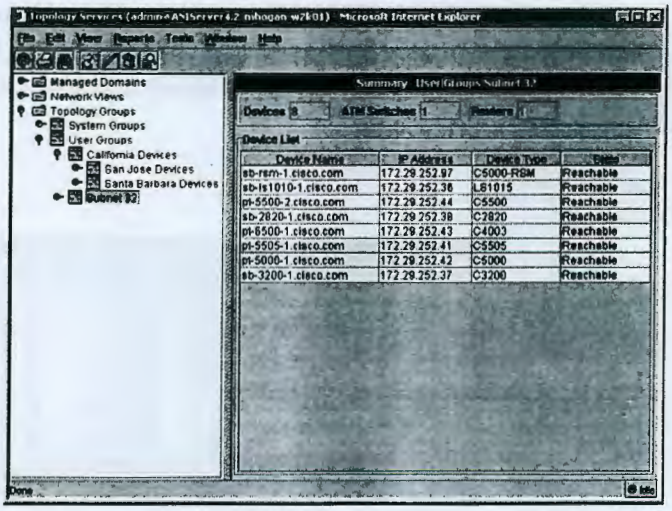


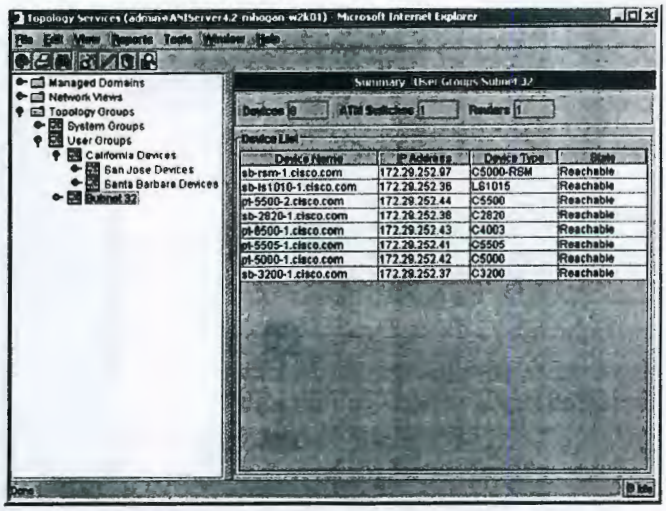
Figure 3
Forming Topology Groups



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

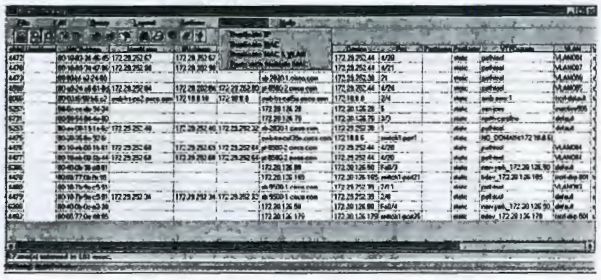
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 468
Doc. 3698

Figure 4
Topology Group in Topology Maps



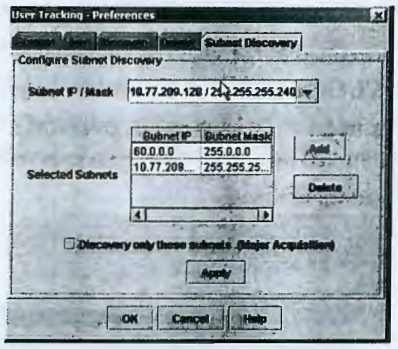
- User Tracking—Designed to assist in locating end-station connections at the access switch, this application is a useful tool in troubleshooting or connectivity analysis. Through automated acquisition, a table of end-user stations and Layer 2 connection information is constructed. This table can be sorted and queried allowing administrators to easily find users. Users can be identified by name, IP handset, MAC and IP address, as well as the switch port and switch that they are connected, along with VLAN and VTP assignment of the port. Predefined reports, such as duplicate MAC per switch port, or duplicate IP addresses, enable managers to locate mobile users or violations in port policies.

Figure 5
User Tracking



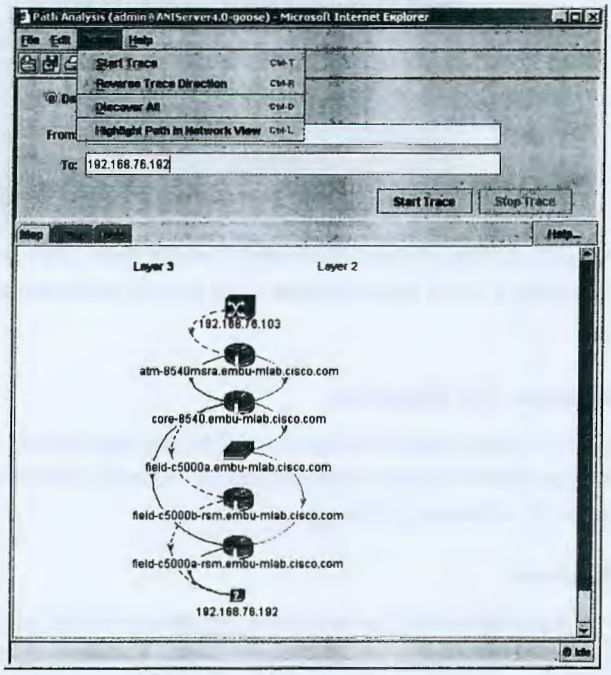
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 6
Subnet based acquisition



- Path Analysis—An application for switched network management, this is an extremely powerful tool for connectivity troubleshooting. Path Analysis utilizes User Tracking, topology services, and real-time spanning tree information to determine Layer 2 and Layer 3 connectivity between two end-points, or IP Handsets, in the network. The resulting trace is presented in graphical topology views that illustrate the Layer 2 and Layer 3 devices, path direction and link types, and in tabular formats that provide specific interface, IP address, VLAN, and link type information.

Figure 7
Path Analysis



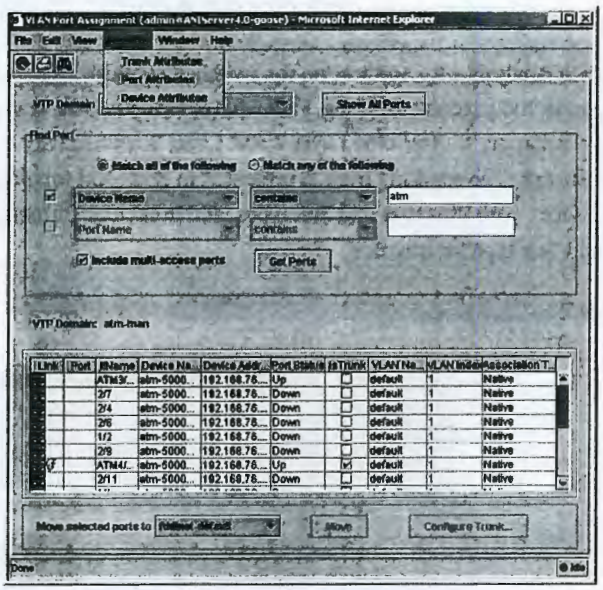
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 469
Doc. 3698

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

Figure 8
VLAN Port Assignment



Campus Manager 3.3 is a must for switched network management, and is an integral piece of the LAN Management Solution, by providing a broad, comprehensive set of tools for managing and administering the entire LAN environment.

Campus Manager 3.3 Features

Campus Manager provides a variety of functions within Topology Services, User Tracking, Path Analysis and VLAN/LANE port assignment that network managers can use to better understand, monitor, configure, diagnose, and be proactive to network infrastructure changes.

Topology Services

Topology Services provides access to a wide variety of physical and logical topology maps, summary lists of devices, ports, and their network relationships. Topology Services also acts as the launching point for topology-related configuration and diagnostic tools.

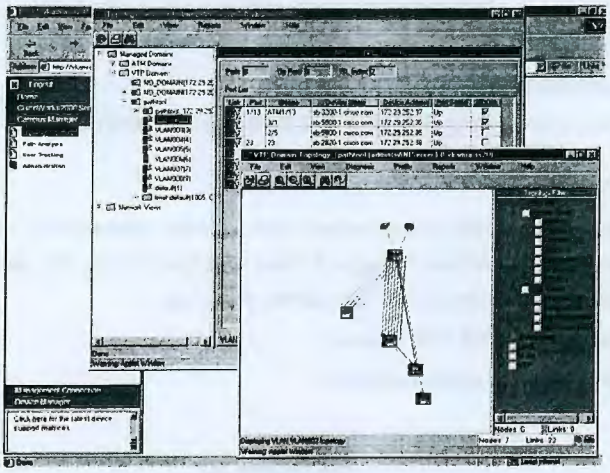
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

In Campus Manager 3.3, network topology maps can be displayed in a variety of ways from both a flat Layer 2 to abstracted views that better represent and scale to large campus networks. These abstractions are categorized into three different groups: managed domains, network views and topology groups. Managed domains are topological views of logical groups of devices organized around ATM switch fabrics and VTP domains. Network views are physical displays of the network and are organized to provide full and abstracted views, such as LAN edge views, Layer 2 views, unconnected device views, and VTP views. Topology Groups are custom views that are a subset of the entire network based on the group rule defined while creating the view. They are can be two types of groups—system defined groups that are custom views created by admin user and user defined views which are created by CiscoWorks users. Membership to these groups are made via rules that can be evaluated either automatically or upon user request and these groups help in generating custom views that are a subset of the Layer 2 views.

Key features in the Campus Manager topology services include:

- Autodiscovery and display of Cisco switches, routers, and probes using the Cisco Discovery Protocol (CDP) and SNMP
- Display of physical and logical Layer 2 connections within the discovered LAN environment
- Highlighting tools to identify specific classes of devices or links such as switches, route switch modules (RSMs), Fast Ethernet, EtherChannel®, ATM links, Cisco Customer Response Applications, and other relevant Cisco device elements
- Expanded scalability to support more than 2000 Cisco devices
- Display of multilayer switches and components (switching entities and route-processing entities) with the ability to highlight logical relationships between devices, such as flow masks and shortcuts
- Device status indicators on the topology maps based on CDP, ILMI, ELMI, and SNMP availability
- Automated discrepancy reporting during discovery highlights connection problems, link mismatches, and logical misconfigurations
- Graphical interface for creating VLAN and LANE services for Ethernet, Token Ring, and transparent VLANs
- Graphical interface for locating—through search parameters—and assigning switch ports individually or in bulk to a VLAN
- ATM soft PVC configuration and diagnostics

Figure 9
Topology Views and Tools



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 470
Doc. 3698

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

VLAN management services provide:

- Tabular summary views of VLANs shows participating ports, devices, links, and port status information
- Graphical setup of VLANs (including transparent VLANs) and VLAN membership to simplify administration
- Integration of LANE configuration services in VLAN configuration tools for more efficient operational and engineering practices
- A separate interface for administrators to quickly search, using a variety of criteria, and assign selected switch ports, individually or in bulk, to VLANs
- Logical display of VLAN configurations makes it easy to visualize switch connections
- Automated discrepancy reports highlight connection problems and link mismatches
- Automated VLAN membership registration reduces administration and configuration requirements

ATM Management

Campus Manager offers a graphical tool for managing complex ATM networks, simplifying configuration and performance monitoring. ATM networks are displayed on the topology map and the logical VLAN and ATM domain views provide graphical representations of ATM switches and LANE elements. "Drill down" capability allows access to configuration and performance monitoring tools. ATM management functions include:

- Autodiscovery of ATM switches, including switched virtual circuit (SVC) and PVC connections
- Connectivity checking of SVC and PVC connections
- End-to-end virtual circuit path tracing and analysis, which assists in connectivity diagnostics
- LANE troubleshooting and performance analysis
- Quality of service (QoS) templates for simplifying the configuration of typical traffic such as video or constant-bit-rate (CBR)
- Simple configuration of soft PVCs
- ATM remote monitoring (RMON) data collection and analysis

User Tracking

User Tracking automatically locates servers and end-user workstations, and Cisco voice over IP (VoIP) telephone handsets and their connections to Layer 2 Cisco switches. During this discovery process it also tabulates specific connection information about that end station, including:

- VLAN name, type, and VTP domain
- Switch port number, name, and state

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

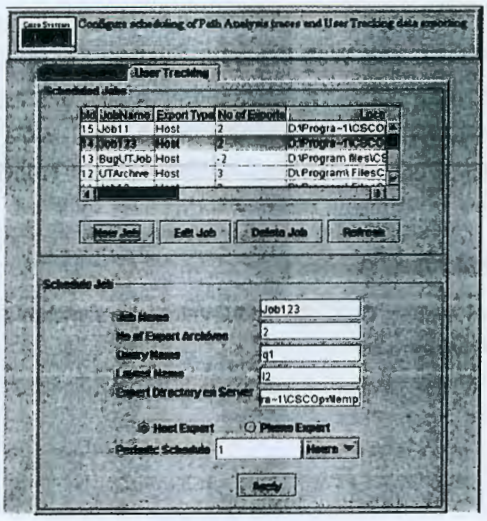
- MAC and IP address of the end station and its subnet
- Tabular and sortable listing of all switch port attached end-user workstations, servers and IP handsets
- Last-seen time stamp reflecting last acquisition in which the end station was detected
- User login name passed automatically from the Windows NT Primary Domain Controller or Novell Directory Structure, or from the UNIX host

Campus Manager simplifies the dynamic nature of many business environments by providing a large number of sortable parameters that can be used to locate end-user stations. User Tracking discovers end stations connected to switch ports automatically and provides a means to identify end users, their assigned VLANs, and host station connections. User Tracking also supports voice/data convergence with interfaces to Cisco CallManager for correlating the IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users.

User Tracking provides the following features:

- Enhanced scalability to support 60,000 end stations
- Predefined reports that identify duplicate MAC and IP addresses, ports with multiple MAC addresses and duplicate sysnames.
- IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users
- Tabular and sortable listing of all switch port-attached end-user workstations and IP handsets
- Customized tables for user-defined, detailed reporting
- GUI for user tracking information table configuration to support dynamic/mobile users
- Scheduling managers for automating address change updates
- Easy-to-use search utility box locating users by MAC addresses, IP addresses, DNS host names, switch port labels, and optional voice handsets
- Provides ability to schedule User Tracking. Also exports User Tracking reports.
- Ability to define acquisition based on a subnet range

Figure 10
Scheduled export of User Tracking Reports



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 471
Doc. 3698

Path Analysis

Path Analysis is a powerful diagnostic tool for determining the Layer 2 and Layer 3 path between two selected endpoints using Campus Manager-discovered end-station data, VLAN/LANE configuration information, real-time Layer 3 path trace information, and spanning-tree calculations. Displays of path information are available in both topological map and tabular displays. Key Path Analysis features include:

- View the Layer 2 and Layer 3 path information in a map format with traces showing end stations, Layer 2 and 3 devices, route directions, and cut-through paths
- View specific details of the Layer 2 and Layer 3 path, including IP addresses and interfaces traveled, VLAN and VTP domain names, and port speeds and duplex settings
- Perform traces immediately or schedule them
- Perform traces using IP address, DNS name, or by telephone number for voice calls as start/stop points
- Provide Layer 2 and Layer 3 trace information between Cisco voice elements using interfaces to call detail records for specific voice calls
- Provides ability to schedule path traces. Also exports path traces data.

Built on the CiscoWorks Management Server

The CiscoWorks management server provides common resources, such as Web services, discovery, shared databases and database services, and the management desktop. Cisco Management Connection, a service on the CiscoWorks2000 server, delivers a set of tools for integrating applications into the management desktop using Internet-based standards and technologies. These tools allow users to link Web-based management applications to the CiscoWorks family of products and application developers to easily link Web-based applications through a certified registration mechanism. Cisco Management Connection has been used by Cisco and more than 30 network management vendors, including Hewlett-Packard, Computer Associates, Sun Microsystems, and Tivoli Systems to create certified Cisco Management Connections for their applications. This rapid adoption has created an environment in which users can easily build management intranets that link together their favorite Web-based management applications.

Specifications

Server, Client, and Web Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco Devices

Most Cisco routers, Catalyst® and LightStream switches, as well as Cisco AVVID devices. Contact your Cisco representative for a complete list.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Supported Cisco IOS Versions

- Cisco IOS® version 10.3 and above
- Catalyst Supervisor code 2.1 and above

Availability

Campus Manager 3.3 is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on Campus Manager, see:
http://cisco.com/warp/public/cc/pd/wr2k/

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203046/ETMG_03/03

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 472
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 473
Doc. 3698

E C T
9370
CPL - AC

rp24xx Hardware Manual

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 474
3698
Doc.

Notice

Hewlett-Packard makes no warranty of any kind with regard to this material, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

All rights are reserved. No part of this document may be photographed, reproduced, or translated to another language without prior written consent of Hewlett-Packard Company.

The information contained in this document is subject to change without notice.

1 What's New, and Using This Information

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 475
3698
Doc.

Using rp24xx Server Information

This site contains hardware support information pertaining to Hewlett-Packard rp24xx Servers. In the frame on the left side of your screen, you will see a general navigation network in a Table of Contents format. Click on the plus (or "add") sign (+) next to any topic to view the sub-topics within.

The topics were developed to support hardware-related tasks that you may need to perform in order to prepare for delivery, unpacking, installation, operation, or adding components to your rp24xx server.

There are several ways to navigate this site. The left frame will usually contain the main navigation network. The initial view in this frame is similar to a Table of Contents. However, if you wish to view a listing by topic, click on the "Index" button near the top of the screen.

Some of the topics will link to information at another site. If you are reading this information from a CD-ROM, you will need internet access to complete those links.

If you prefer to navigate this site in a more "linear" way, find the task you wish to perform, then click on that link. At the bottom of the content frame, you will see the navigation instructions to the next "logical" piece of information along with the previous "logical" piece of information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 476
3698
Doc.

What's New?

Visit this page to find out what new rp24xx server information has been released since the last web site and CD-ROM publish. The additions and modifications listed here are effective as of August 2002.

New Sections:

"What's New?" is the latest addition to the rp24xx server web site. This section will tell you about the latest changes to the previously-released information and provide a direct link to that information.

Modified Sections:

- Identified changes to all sections as applicable to HP e3000.

NOTE All references to rp24xx are equally applicable to the HP e3000.

ECT
236
DEC
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 477
3698
Doc.

E C T
9260
AC

2 System Hardware Overview and Reference Information

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.: Nº 478
3698
Doc.

System Overview

Hardware Overview

For an overview of the Enterprise Server Family hardware -

http://www.hp.com/products1/servers/family_overview.html

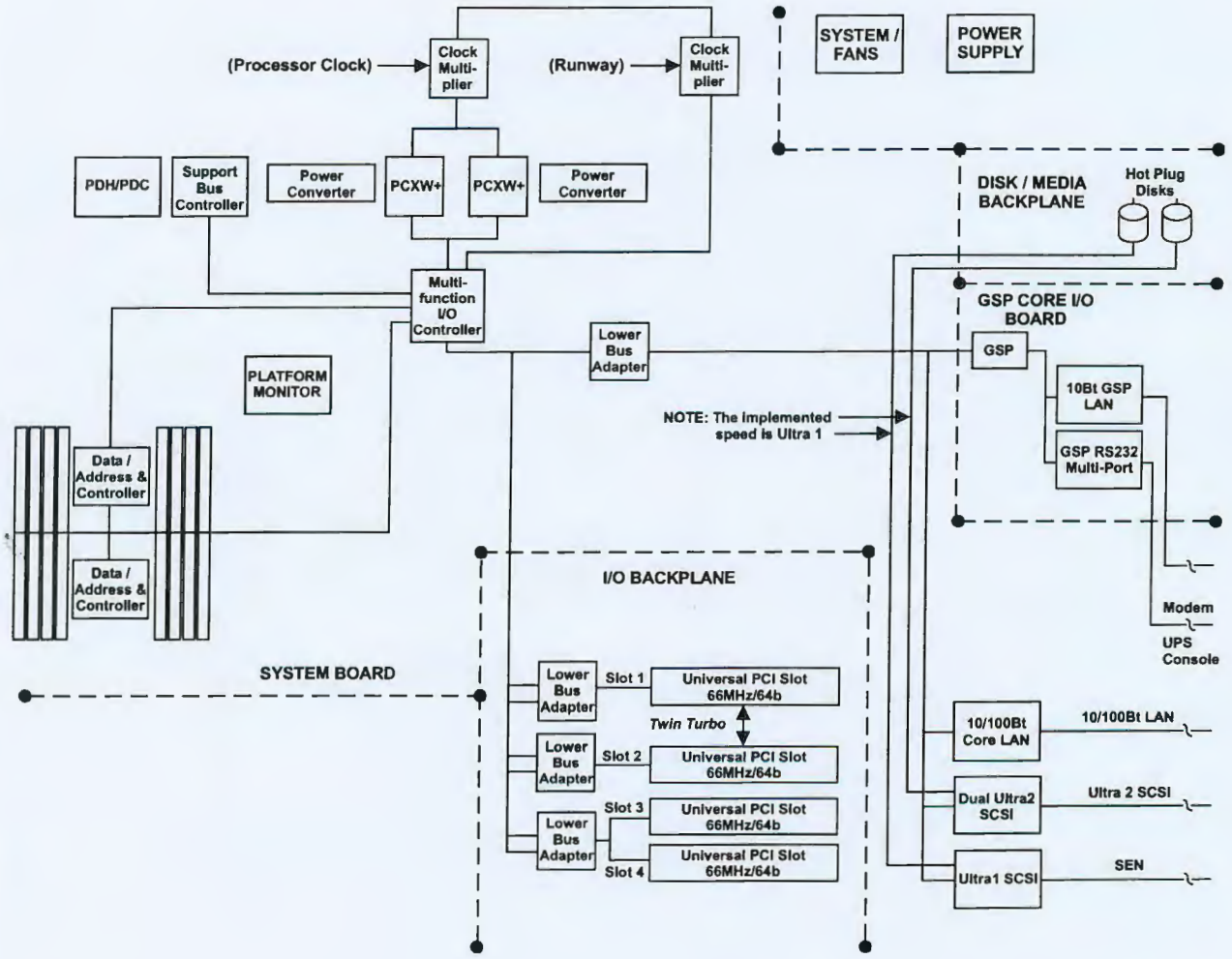
For an overview of the HP-9000 rp24xx Server hardware -
http://www.unixsolutions.hp.com/products/servers/aclass/index.htm

Software Requirements

rp24xx servers are designed to operate with HP-UX version 11.ACE or later.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 479
3698
Doc.

rp24xx Block Diagram



ccrr016

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 480
Doc. 3698

hp Server rp24xx Safety and Regulatory Information

Overview

Regulatory Compliance statements are required by some countries for international importation of rp24xx Servers. The following information is provided:

- Regulatory Information
- Electrical Safety
  - Electrostatic Discharge (ESD) Precautions
  - Battery Notice
- Cabinet Safety Precautions
- Declaration of Conformity
- FCC Statement (USA Only)
- Canada RFI Statement
- European Union RFI Statement
- Korean RFI Statement
- Taiwan RFI Statement
- Japan Safety and Regulatory Statements
- Acoustics (Germany)
- Australian C-Tick Label
- Laser Safety

Product Information

For detailed information on the rp24xx Enterprise Server product, please go to the http://docs.hp.com web site (in the Systems Hardware selection).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 481
Doc. 3698

Regulatory Information

For your protection, this product has been tested for conformance to various national and international regulations and standards. The scope of this regulatory testing includes electrical and mechanical safety, electromagnetic emissions, immunity, acoustics and hazardous materials.

When required, approvals are obtained from third party test agencies. Approval marks appear on the product label. In addition, various regulatory bodies require some information under the headings listed in this section.

Electrical Safety

This product has not been evaluated for connection to an "IT" power system (AC distribution system having no direct connection to earth according to IEC 950).

Locate the AC outlet near the computer! The AC power cords are this product's main AC disconnect devices and must be easily accessible at all times.

Electrostatic Discharge (ESD) Precautions

When handling any electronic component or assembly (such as, a PCI card or Memory SIMM), you must observe the following antistatic precautions to prevent damage. An ESD kit (HP P/N A3024-80004) is available (or supplied with Memory additions). This kit contains one wrist strap, one conductive sheet, and one anti-static foam pad.

- Always wear a grounded wrist strap when working around the system, and when handling printed circuit boards.
- Treat all assemblies, components and interface connections as static-sensitive.
- Avoid working in carpeted areas, and keep body movement to a minimum while removing or installing boards, to minimize buildup of static charge.

Battery Notice

This product contains two Lithium batteries located on the:

- System Board
- Guardian Service Processor board

These batteries are not to be removed or replaced by the user. If either battery needs to be replaced, contact your Hewlett-Packard authorized service personnel.

CAUTION Lithium batteries may explode if mistreated.
Do not recharge, disassemble, or dispose of in a fire.

Please properly recycle all used batteries.

Cabinet Safety Precautions

WARNING **Cabinets are heavy even when empty. Exercise caution when moving cabinets whether equipment is installed in the cabinet or not. Avoid rolling cabinets on rough or uneven surfaces or inclines greater than 10 degrees. Unloading cabinets from the pallet and movement of cabinets should be performed by at least two people.**

WARNING **Slideable products are not to be extended from the cabinet while the equipment is on the shipping pallet. The cabinet must be unloaded from the pallet and both front and rear anti-tip feet properly installed prior to extending any slideable product.**

WARNING **Once installed, both the front and rear anti-tip feet must remain in place to maintain stability. Only one slideable product must be extended at a time.**

WARNING **Use of any slide mount product requires the installation of a cabinet anti-tip device.**

The anti-tip device for the following cabinet products is a pair of anti-tip feet: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, and J1502A.

Install both front and rear anti-tip feet on the cabinet before installing any slide mount product.

The anti-tip device for the following cabinets is the installation of ballast in the bottom of the cabinet: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, and C2787A.

To determine ballast requirements, refer to the ballast worksheets in documentation accompanying the cabinet or http://www.hp.com/enclosures/c_rocs.htm

Failure to follow these precautions can result in damage to equipment or injury to personnel

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 482
Doc.

Sicherheitsvorkehrungen für Einbaugehäuse

WARNING **Einbaugehäuse haben auch ohne Inhalt ein hohes Gewicht. Seien Sie also vorsichtig, wenn Sie ein Gehäuse hin und her bewegen, sei es mit oder ohne installierten Innenteilen. Rollen Sie das Gehäuse nach Möglichkeit nicht über rauhe oder unebene Oberflächen bzw. Oberflächen mit mehr als 10 Grad Neigung. Das Abladen von der Palette und Positionieren muß von mindestens zwei Personen durchgeführt werden.**

WARNING **Ziehen Sie keine beweglichen Teile heraus, solange sich das Einbaugehäuse auf der Palette befindet. Laden Sie es zunächst von der Palette ab, und stellen Sie es mit den kippsicheren Vorder-und Hinterfüßen ordnungsgemäß auf, um bewegliche Teile sicher herausziehen zu können.**

WARNING **Nach deren Installation dürfen die kippsicheren Füße nicht wieder entfernt werden, um sicheren Stand zu gewährleisten. Ziehen Sie jeweils nur ein bewegliches Teil heraus.**

WARNING **Bevor Sie auf Gleitschienen ruhende Produkte einbauen, müssen Sie für die Kippsicherheit der Einbaugehäuse sorgen.**

Bei den folgenden Gehäuseprodukten verwenden Sie dazu in Paaren gelieferte kippsichere Füße: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A und J1502A.

Installieren Sie sowohl die vorderen als auch die hinteren kippsicheren Füße, bevor Sie auf Gleitschienen ruhende Produkte einbauen.

Bei folgenden Einbaugehäusen wird die Kippsicherheit erzielt, indem der Schrank unten mit Ballast beschwert wird: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A und C2787A.

Den erforderlichen Ballast können Sie den entsprechenden Arbeitsblättern in der Dokumentation zum Einbaugehäuse entnehmen. Außerdem finden Sie diese Informationen unter www.docs.hp.com

Eine Mißachtung dieser Sicherheitsvorkehrungen kann zu Verletzungen des Personals oder Schäden an den Geräten führen.

ECT 0257 CPL-AC

Consignes de sécurité relatives aux armoires

WARNING **Une armoire est lourde même lorsqu'elle est vide. Faites preuve de prudence lorsque vous en déplacer une, peu importe si des éléments y sont installés ou non. Évitez de faire rouler l'armoire sur un sol irrégulier ou incliné à plus de 10 degrés. Il faut au moins deux personnes pour décharger une armoire de la palette d'expédition et la déplacer.**

WARNING **Ne faites pas glisser les éléments coulissants hors de l'armoire alors qu'elle se trouve sur la palette d'expédition. Vous devez d'abord décharger l'armoire de la palette et installer correctement les pieds antibasculement, en avant et en arrière, avant de faire glisser les éléments coulissants.**

WARNING **Lorsqu'ils sont installés, les pieds antibasculement situés à l'avant et à l'arrière doivent tous deux rester en place pour assurer la stabilité de l'armoire. Vous ne devez faire glisser hors de l'armoire qu'un seul élément coulissant à la fois.**

WARNING **L'utilisation d'un élément coulissant exige l'installation préalable d'un dispositif antibasculement.**

Pour les armoires A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A et J1502A, ce dispositif consiste en une paire de pieds antibasculement.

Fixez les pieds antibasculement à l'avant et à l'arrière de l'armoire avant d'installer un élément coulissant dans cette dernière.

Pour les armoires A1896A, A1897A, A1883A, A1884A, C2785A, C2786A et C2787A, le dispositif antibasculement consiste en un contrepoids que vous devez installer au bas de l'armoire.

Pour connaître le type de contrepoids à utiliser, consultez les feuilles de travail sur les contrepoids dans la documentation qui accompagne l'armoire ou visitez le site www.docs.hp.com

Vous devez prendre ces précautions afin d'éviter des risques de dommage au matériel ou de blessure.

Medidas de seguridad para armarios

WARNING **Los armarios son pesados aun cuando estén vacíos. Tenga cuidado cuando mueva los armarios independientemente de que haya equipo instalado en el armario o no. Evite desplazar los armarios sobre superficies rugosas o disparejas o pendientes de más de 10 grados. Dos personas, como mínimo, tienen que realizar la descarga de los armarios de la plataforma de carga y mover los armarios.**

RQS nº 03/2005 - CN
CPMI - CORREIOS
483
Fls. Nº 4856
Doc. 3698

WARNING **Los productos deslizables no deben extenderse del armario cuando el equipo se encuentre en la plataforma de carga. Se debe descargar el armario de la plataforma e instalar bien las punteras delanteras y traseras de protección antes de extender cualquier producto deslizable.**

WARNING **Una vez instalado, se deberán dejar puestas las punteras de protección, delanteras y traseras, para mantener la estabilidad. Se deberá extender un solo producto deslizable cada vez.**

WARNING **El uso de cualquier producto de montaje deslizable requiere la instalación de un dispositivo de protección del armario.**

El dispositivo de protección para los siguientes armarios es un par de punteras de protección: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A y J1502A.

Instale las punteras de protección delanteras y traseras en el armario antes de instalar ningún producto de montaje deslizable.

El dispositivo de protección para los siguientes armarios es un lastre que se instala en la parte inferior del armario: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A y C2787A.

Para determinar los requisitos de lastre, consulte las hojas de datos del lastre en la documentación suministrada con el armario o bien visite www.docs.hp.com

El incumplimiento de estas medidas de precaución puede tener como resultado daños al equipo o lesiones personales.

ECT
CPL - AC

Procedimentos de Segurança - Armários

WARNING **Os armários são pesados, mesmo quando vazios. Tenha cuidado ao movimentar os armários, quer haja equipamentos instalados quer não. Evite deslizar os armários sobre superfícies acidentadas, irregulares ou com inclinação superior a 10 graus. A retirada dos armários do palete e sua movimentação deverão ser feitas por, no mínimo, duas pessoas.**

WARNING **Partes deslizantes não deverão ser abertas enquanto o armário encontrar-se no palete de embarque. O armário deve ser descarregado do palete e os anteparos nos pés dianteiros e traseiros devem ser instalados adequadamente antes de se abrir qualquer parte deslizante.**

WARNING **Uma vez instalados, tanto os anteparos nos pés dianteiros quanto nos traseiros devem permanecer em seus lugares adequados para garantir a estabilidade da peça. Deve-se abrir apenas uma parte deslizante por vez.**

WARNING **O uso de qualquer produto de montagem deslizante requer a instalação de um dispositivo anti-tombamento para armários.**

Um par de pés anti-tombamento é o dispositivo anti-tombamento para os seguintes armários: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, e J1502A.

Instalar ambos os pés anti-tombamento na frente e atrás do armário antes da instalação de qualquer produto de montagem deslizante.

A instalação de um lastro no fundo do armário é o dispositivo anti-tombamento para os seguintes armários: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, e C2787A.

Para determinar os requisitos de lastro, referir-se a planilha de lastro na documentação que acompanha o armário ou em www.docs.hp.com

A não observância destas precauções pode resultar em danos ao equipamento ou lesões as pessoas.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 484
Doc. 3698

Precauzioni di siccurezza sugli armadi

WARNING **Gli armadi sono molto pesanti anche quando sono vuoti. Esercitare la massima cautela durante lo spostamento degli armadi indipendentemente dal fatto che l'apparecchiatura sia installata o meno. Evitare di far scorrere gli armadi su superfici irregolari, disagevoli o con un'inclinazione superiore ai 10 gradi. Servirsi di almeno due persone sia per scaricare che per spostare gli armadi dal pallet.**

WARNING **Non aprire o estendere gli elementi scorrevoli dagli armadi mentre l'apparecchiatura è sul pallet di trasporto. Prima di estendere o aprire un qualsiasi elemento scorrevole è necessario aver scaricato gli armadi dai pallet ed aver debitamente installato gli appositi piedini antiribaltamento anteriori e posteriori.**

WARNING **Non smontare i piedini antiribaltamento dopo l'installazione perché stabilizzano gli armadi. Estendere o aprire soltanto un prodotto scorrevole per volta.**

WARNING **L'uso di qualsiasi elemento scorrevole richiede l'installazione di un dispositivo antiribaltamento.**

Il dispositivo di questo tipo adatto per i seguenti armadi è costituito da una coppia di piedini antiribaltamento: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A e J1502A.

Installare gli appositi piedini antiribaltamento anteriori e posteriori sull'armadio prima di procedere all'installazione di qualsiasi elemento scorrevole.

Il dispositivo antiribaltamento adatto per i seguenti armadi è costituito dall'installazione di un contrappeso sul fondo dell'armadio: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A e C2787A.

Per determinare i requisiti del contrappeso, fare riferimento alle schede tecniche relative comprese nella documentazione fornita con l'armadio o accedere al sito Web www.docs.hp.com

La mancata applicazione di queste norme precauzionali potrebbe causare danni all'apparecchiatura o incidenti al personale.

Säkerhetsföreskrifter för kabinett

WARNING **Kabinetten är tunga även när de är tomma. Var försiktig när du flyttar ett kabinett, oavsett om det är tomt eller innehåller utrustning. Undvik att rulla kabinett på ett underlag som är ojämnt eller lutar mer än 10 grader. Det krävs minst två personer för att lasta av ett kabinett från transportpallen eller för att flytta det.**

WARNING **Inskjutningsbara produkter får inte vara utdragna när utrustningen befinner sig på transportpallen. Kabinettet måste lastas av från pallen och tippskyddsfötter ska monteras både fram- och baktill innan en inskjutningsbar produkt dras ut.**

WARNING **Efter montering ska tippskyddsfötterna sitta kvar både fram- och baktill så att stabiliteten upprätthålls. De inskjutningsbara produkterna får bara dras ut en i sänder.**

WARNING **Kabinettet måste tippskyddas för att en inskjutningsbar produkt ska kunna användas.**

För följande kabinettprodukter ska två tippskyddsfötter användas: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A och J1502A.

Installera både den främre och den bakre tippskyddsfoten på kabinettet innan du installerar en inskjutningsbar produkt.

Följande kabinett tippskyddas genom att ballast placeras i kabinettets botten: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A och C2787A.

I kabinettets dokumentation finns specifikationer för ballast. Du kan också gå till www.docs.hp.com

Om dessa föreskrifter inte följs föreligger risk för personskada eller skada på utrustningen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 485
Doc. 3698

Voorzorgsmaatregelen voor de veiligheid voor kasten

WARNING **Kasten zijn zwaar, ook als deze leeg zijn. Ga voorzichtig te werk als u een kast verplaatst, of er nu wel of niet apparatuur in de kast is geïnstalleerd. Rol kasten niet over ruwe of ongelijke oppervlakken of hellingen van meer dan 10 graden. Als u een kast van een pallet moet afhalen of moet verplaatsen, doet u dat dan altijd met twee personen.**

WARNING **Zorg ervoor dat er geen uitschuifbare onderdelen uit de kast uitsteken als de apparatuur ter verzending op een pallet is geplaatst. Voordat u een uitschuifbaar onderdeel uitschuift, moet u de kast eerst van het pallet halen en de stabilisatiesteunen aan de voor- en achterkant op de juiste manier installeren.**

WARNING **Zodra de kast is geïnstalleerd, mogen de stabilisatiesteunen niet meer worden verplaatst. U mag niet meer dan één uitschuifbaar onderdeel tegelijk uitschuiven.**

WARNING **Als u verwisselbare opslagmedia wilt plaatsen, moet u de kast stabiliseren.**

Voor de volgende producten maakt u gebruik van stabilisatiesteunen: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A en J1502A.

U moet de stabilisatiesteunen zowel aan de voorkant als aan de achterkant van de kast aanbrengen voordat u verwisselbare opslagmedia plaatst.

De volgende kasten moet u stabiliseren door onderin de kast ballast te plaatsen: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A en C2787A.

Raadpleeg de informatie over ballast in de documentatie die u bij de kast heeft ontvangen of bezoek www.docs.hp.com om te bepalen hoeveel ballast is vereist.

Als u deze aanwijzingen niet opvolgt, kan dit leiden tot schade aan de apparatuur of lichamelijk letsel.

Sikkerhedsforanstaltninger for skabe

WARNING **Skabene er tunge, selv når de er tomme. Vær forsigtig når De flytter skabe, hvad enten der er installeret udstyr i skabet eller ej. Undgå at rulle skabe på ru eller ujævne overflader eller skråninger der hælder mere end 10 grader. Der skal mindst to personer til at aflæsse skabe fra pallen og til at flytte skabe.**

WARNING **Udtræksdele må ikke være trukket ud, når skabet står på forsendelsespallen. Skabet skal først læsses af pallen og anti-tip fødderne skal være installeret både forpå og bagpå, før udtræksdelene må trækkes ud.**

WARNING **Efter installation skal både de forreste og bageste anti-tip fødder blive siddende for at opretholde stabiliteten. Der må kun trækkes en udtræksdel ud ad gangen.**

WARNING **Ved enhver brug af udtræksdele skal der monteres anti-tip indretninger for skabet.**

For følgende skabstyper anvendes der som anti-tip indretning et par anti-tip fødder: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A og J1502A.

Anti-tip fødderne skal monteres både på for- og bagsiden, før der isættes udtræksdele.

For følgende skabe anvendes der som anti-tip indretning en ballast i bunden af skabet: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A og C2787A.

For beslutningen om, hvorvidt der er brug for ballast, henvises til ballasttegningerne i papirerne, der følger med skabet, samt tit www.docs.hp.com

Hvis ovenstående anvisninger ikke følges, kan det medføre materiel skade eller kvæstelse.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 486
Doc. 3601

Sikkerhetsforanstaltninger for skapene

WARNING **Skapene er tunge, selv når de er tomme. Vær forsiktig når du flytter skap, uansett om de er tomme eller inneholder utstyr. Ikke rull skap på ru eller ujevne overflater eller i skråninger som heller mer enn 10 grader. Det trengs minst to personer til lessing av skap fra pallen og til flytting av skap.**

WARNING **Produkter som kan gli inn og ut av skapet bør ikke være trukket ut når skapet er på transportpallen. Skabet må lesses av pallen og anti-tippe-føtter må være påmontert både foran og bak før et produkt som kan gli inn og ut av skapet, trekkes ut.**

WARNING **Etter montering skal anti-tippe-føttene både foran og bak fortsatt være på for å opprettholde stabilitet. Produkter som kan gli inn og ut av skapet, må kun trekkes ut ett og ett om gangen.**

WARNING **Bruk av produkter som kan gli inn og ut, krever at det installeres en anti-tippe-enhet for skap.**

Anti-tippe-enheten for følgende skapprodukter er et par anti-tippe-føtter: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A og J1502A.

Installer både fremre og bakre anti-tippe-fot på skapet før du installerer produkter som kan gli inn og ut.

Anti-tippe-enheten for følgende skap er installering av ballast nederst i skapet: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A og C2787A.

Når du skal bestemme kravene til ballast, kan du se i ballastbeskrivelsen i dokumentasjonen som fulgte med skapet, eller gå til www.docs.hp.com
Hvis disse forholdsreglene ikke blir fulgt, kan det føre til skade på utstyr eller personer.

Laitekaappia koskeva turvavaroitus

WARNING **Kaapit ovat tyhjinäkin painavia. Ole varovainen siirtäessäsi kaappia siitä riippumatta, onko siihen asennettu laitteistoa. Älä rullaa kaappeja karkeilla tai epätasaisilla pinnoilla tai jos pinnan kaltevuus ylittää 10 astetta. Kaappien ottamiseen alas lastausalustalta ja niiden siirtämiseen tarvitaan ainakin kaksi henkilöä.**

WARNING **Liukuvia osia ei pidä vetää ulos kaapista laitteen ollessa lastausalustalla. Kaappi täytyy ottaa alas alustalta, ja sekä etummaisen että takimmaisen kallistustuen täytyy olla asennettu ennen liukuvien osien vetämistä ulos.**

WARNING **Kun kallistustuet on asennettu, ne täytyy jättää paikoilleen sekä edessä että takana, jotta kaappi pysyisi vakaasti paikoillaan. Vain yksi liukuosa saa olla ulkona kerrallaan.**

WARNING **Liukuviksi asennettavien tuotteiden käyttö vaatii laitekaapin kaatumisen estävän laitteen asentamista.**

Kaatumisen estävä laite laitekaapeille A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A ja J1502A on pari kaatumisen estäviä jalkoja.

Asenna sekä etu- että takajalka laitekaappiin ennen liukuviksi asennettavien tuotteiden asentamista.

Kaatumisen estävänä laitteena laitekaapeille A1896A, A1897A, A1883A, A1884A, C2785A, C2786A ja C2787A toimii painolastin asentaminen laitekaapin pohjalle.

Sopivan painolastin määrittämiseksi tutustu tuotteen mukana tulleisiin ohjeisiin (ballast worksheets) tai käy www-sivuilla osoitteessa http://www.docs.hp.com

Näiden ohjeiden noudattamatta jättäminen voi johtaa laitteiston vaurioitumiseen tai ihmisten loukkaantumiseen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 487
Doc. 3698

Меры предосторожности при работе со стойками

ОСТОРОЖНО **Стойка очень тяжелая, даже если в ней не установлено оборудование, поэтому при ее перемещении соблюдайте меры предосторожности. Избегайте перемещения стойки по неровной поверхности или поверхности с углом наклона более 10 градусов. Снятие стойки с поддона и ее перемещение необходимо выполнять по крайней мере вдвоем.**

ОСТОРОЖНО **Оборудование, установленное на полозьях, нельзя выдвигать из стойки, пока она находится на транспортировочном поддоне. Прежде чем выдвинуть из стойки какое-либо оборудование, необходимо снять стойку с поддона и выдвинуть спереди и сзади стойки дополнительные опоры, предохраняющие от опрокидывания.**

ОСТОРОЖНО **Для обеспечения устойчивости стойки передние и задние опоры, предохраняющие стойку от опрокидывания, должны быть всегда выдвинуты. Никогда не выдвигайте одновремеино более одного компонента оборудования, установленного на полозья.**

ОСТОРОЖНО **Перед использованием какого-либо оборудования, установленного на полозьях, необходимо установить устройство, предохраняющее стойку от опрокидывания.**

Для стоек A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A и J1502A таким устройством являются две выдвижные опоры, предохраняющие от опрокидывания.

Прежде чем устанавливать на полозьях какое-либо оборудование, установите спереди и сзади стойки опоры, предохраняющие от опрокидывания.

Для стоек A1896A, A1897A, A1883A, A1884A, C2785A, C2786A и C2787A в качестве устройства, предохраняющего от опрокидывания, используется балласт, который устанавливается внизу стойки.

Требования к балласту см. в документации, прилагаемой к стойке, или на Web-узле по адресу: www.docs.hp.com

Несоблюдение этих мер предосторожности может привести к травмам персонала и повреждению оборудования.

キャビネットの転倒防止

注意 キャビネットは空の状態でも相当の重量があります。キャビネットに装置が搭載されていてもいなくても、移動には充分注意してください。表面に凹凸があったり水平でない場所では、キャビネットを回転したり１０度以上傾斜させることは避けてください。パレットからキャビネットを降ろしたり移動するときは最低２人以上で行ってください。

注意 装置が輸送パレットの上にある間は、スライド型製品はキャビネットの外に引き出さないでください。スライド型製品をキャビネットから引き出しておく場合は、事前にキャビネットをパレットから降ろし、傾き防止部品を前後両方とも適切に取り付けてください。

注意 設置後は、前後の傾き防止部品は安定を維持するため、取り付けたままの状態にしておいてください。スライド型製品は、一度に２台以上引き出さないでください。

警告 スライド型製品をキャビネットに組み込む場合には、あらかじめ傾き防止部品を取り付けてください。

次のキャビネットに使用する傾き防止部品は、１組のアジャスタです。
A4900A、A4901A、A4902A、A5134A、A5135A、A5136A、J1500A、J1501A、J1502A

キャビネットの前と後にアジャスタを取り付けてから、スライド型製品を組み込んでください。

次のキャビネットに使用する傾き防止部品は、キャビネットの底に取り付けるバラスト（重り）です。
A1896A、A1897A、A1883A、A1884A、C2785A、C2786A、C2787A

必要なバラストを調べるには、キャビネット付属の説明書にあるバラスト・ワークシートを参照するか、 www.docs.hp.com をご覧ください。

キャビネットに傾き防止部品を取りつけないで、スライド型製品を組み込むと、装置を損傷したりけがをする恐れがあります。

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 488
Doc. 3698

캐비닛 안전 주의사항

경고 캐비닛은 비어 있는 경우에도 무게가 나갑니다. 캐비닛을 운반할 때에는 안에 장비가 설치되어 있지 않더라도 항상 주의하십시오. 캐비닛을 지면에 굴곡이 있거나 수평을 이루지 않는 곳에서 회전하거나, 10 도 이상 경사로 기울이지 마십시오. 운반대서 캐비닛을 내리거나, 운반할 때에는 적어도 2 사람 이상이 수행해야 합니다.

경고 장비가 운반대에 있는 경우, 슬라이드형 제품이 캐비닛 밖으로 빠져 나오지 않도록 주의하십시오. 슬라이드형 제품을 캐비닛에서 꺼내려면, 우선 캐비닛을 운반대서 내리고 수평을 유지하기 위한 고정용 다리를 앞뒤 양쪽에 설치해야 합니다.

경고 설치를 마친 다음, 앞뒤 고정용 다리는 안정성을 위해 그대로 두십시오. 슬라이드형 제품은 한번에 두 개 이상 캐비닛에서 꺼내지 마십시오.

경고 슬라이드형 제품을 캐비닛에 넣을 경우, 수평을 유지하기 위한 장치를 사용하십시오.
다음 캐비닛 제품에 사용하는 수평 유지 장치는 두개의 고정용 다리로 되어 있습니다.
A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, J1502A

캐비닛 앞뒤 양쪽에 고정용 다리를 끼운 다음 슬라이드형 제품을 설치하십시오.

다음 캐비닛 제품에 사용하는 수평 유지 장치는 캐비닛 바닥에 까는 밸러스트입니다.
A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, C2787A

필요한 밸러스트를 보려면, 관련 캐비닛에 있는 설명서에서 밸러스트 리스트를 참조하거나, **www.docs.hp.com** 를 살펴보십시오.

수평 유지 장치를 설치하지 않은 채로 작업을 할 경우 장비가 손상되거나, 운반자가 상처를 입을 수 있습니다.

E C T - CPL - AC

安 全 措 施

注意 空机柜也很沉重。无论机柜里是否装有设备，都要小心移动。不要在粗糙不平处滚动，也不要使机柜倾斜超过 10 度。无论是从货盘上搬下机柜，还是移动机柜，都应当由至少两个人来操作。

注意 当设备放在运输货盘上时，请勿将可滑动的产品从机柜中移出，在移动可滑动的产品之前，一定要先把机柜从货盘上卸下来，并将前后防倾倒支脚装好。

注意 装好前后防倾倒支脚后，机柜应保持稳定不动，每次只能从机柜中移出一件可滑动的产品。

注意 任何滑动安装产品均需要安装机柜防倾倒设备，下列机柜产品的防倾倒设备是一对防倾倒支脚：A4900A、A4901A、A4902A、A5134A、A5135A、A5236A、J1500A、J1501A 和 J1502A。

安装滑动安装产品之前应在机柜上安装前后防倾倒支脚。

下列机柜的防倾倒设备是在机柜底部安装的压载物：A1896A、A1897A、A1883A、A1884A、C2786A 和 C2787A。

要确定是否需要压载物，请参考随机柜一起提供文档中的压载物数据表格，或访问下面网址：www.docs.hp.com

如果不能遵守这些措施将导致设备的损坏或人员的伤亡。

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 489
3698
Doc.

機箱安全措施

注意 機箱即使是空的，也很沉重，無論其中裝有設備與否，都要小心移動。
不要在粗糙不平的地面滾動機箱，也不要讓機箱傾斜超過 10 度。
無論是從運送底座上搬下機箱，還是移動機箱，都應當至少由兩個人來操作。

注意 當設備放在運送底座上時，可滑動的製品不可伸出機箱以外。讓可滑動的製品伸出機箱以前，一定要先把機箱從底座上卸下，並將前後防傾倒腳座裝好。

注意 當裝好後，前後兩個防傾倒腳座須保持這個狀態以維持穩定。一次只能讓一件可滑動的製品伸出機箱以外。

注意 要使用任何滑軌安裝產品前，須要先在機箱上安裝防傾倒裝置。
下列機箱產品的防傾倒裝置是一對防傾倒的機箱腳座：
A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, 及 J1502A

在安裝任何滑軌安裝產品前，請先安裝機箱前後的防傾倒腳座。

下列機箱產品的防傾倒裝置是安裝在機箱底部的壓艙物：
A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, 及 C2787A

要決定須要多少壓艙物，請參考機箱隨附的文件中的壓艙物工作表，或參閱 www.docs.hp.com

不遵循這些安全措施可能會造成設備損毀或人員傷害。

Declaration of Conformity

DECLARATION OF CONFORMITY
according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company
Internet & Applications Systems Division

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747
USA

declares, that the product

Product Name: HP Server rp24xx (where x is any number 0-9)

Regulatory Model: RSVL-0107-A-xx (where -xx is an optional suffix and x is any letter or blank)

Product Options: All

conforms to the following Product Specifications:

Safety: IEC 60950:1991+A1+A2 +A3 +A4 /
EN 60950: 1992+A1+A2 +A3 +A4 +A11
IEC 60825-1:1993 +A1 / EN 60825-1:1994+A11, Class 1
GB 4943-1995

EMC: CISPR 22:1997 / EN 55022:1998 Class A [1)]
CISPR 24:1997 / EN 55024:1998

IEC 61000-3-2:1995 / EN 61000-3-2:1995 +A14
IEC 61000-3-3:1994 / EN 61000-3-3:1995
GB 9254-1988

Supplementary Information

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The product was tested in a typical configuration with Hewlett-Packard computer peripherals.

2) DC versions of the product were tested in a typical configuration with a Hewlett-Packard 6813A AC/DC power source.

Roseville, 11/28/01

Frank D. Dembski Jr., Quality Manager

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 130, D-71034 Böblingen (FAX: + 49-7031-14-3143)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 490
3698
Doc.

FCC Statement (USA Only)

The United States Federal Communications Commission has specified that the following notice be brought to the attention of users of this product:

NOTE This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Hewlett-Packard's system verification tests were conducted with HP-supported peripheral devices and HP shielded cables, such as those you receive with your computer. Changes or modifications not expressly approved by Hewlett-Packard could void the user's authority to operate the equipment. Cables used with this device must be properly shielded to comply with the requirements of the FCC.

Canada RFI Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Notice relative aux interférences radioélectriques (Canada)

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union RFI Statement

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

E.C.T.I. CPL FAC

Korean RFI Statement

사용자 안내문 (A급 기기)

이 기기는 업무용으로 전자파 적합 등록을 받은 기기이오니, 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Taiwan RFI Statement

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japan Safety and Regulatory Statements

高調波ガイドライン適合品

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

省エネ法による区分：K

エネルギー消費効率：0.29

エネルギー消費効率とは，省エネ法で定める測定方法により測定された消費電力を，省エネ法で定める複合理論性能で除したものである。

省エネ法による区分：G

エネルギー消費効率：0.41

エネルギー消費効率とは，省エネ法で定める測定方法により測定された消費電力を，省エネ法で定める複合理論性能で除したものである。

RQS nº 03/2005 - CN
CPMI - CORREIOS
491
Fls. Nº
Doc. 3008

Acoustics (Germany)

Acoustic noise level per ISO 9296 (25° C):

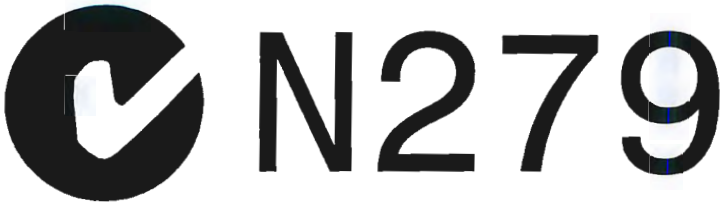
LpA_m <60dB (operators position)

Geräuschemission (Deuschland)

Geräuschemission nach ISO 9296 (25° C):

LpA_m <60dB (Arbeitsplatz)

Australian C-Tick Label



Laser Safety

This product contains a laser internal to the Optical Link Module (OLM) for connection to the Fibre communications port.

In the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. The certification is indicated by a label on the plastic OLM housing.

Outside the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in IEC 825-1:1993 and EN 60825-1:1994, including Amendment 11:1996.

ECT
CPL AC

ESD Safety Standards

Static charges (voltage levels) occur when objects are separated or rubbed together. The voltage level of a static charge is determined by the following factors:

- Types of materials
- Relative humidity
- Rate of change or separation

Effect of humidity on ESD charge levels

The following table lists charge levels based on personnel activities and humidity levels.

Activity[a]	Humidity[b] and charge levels (voltages)[c]			
	26%	32%	40%	50%
Person walking across a linoleum floor	6,150 V	5,750 V	4,625 V	3,700 V
Person walking across a carpeted floor	18,450 V	17,250 V	13,875 V	11,100 V
Person getting up from a plastic chair	24,600 V	23,000 V	18,500 V	14,800 V

a. Source: B.A. Unger, Electrostatic Discharge Failures of Semiconductor Devices (Bell Laboratories, 1981)
b. For the same relative humidity level, a high rate of airflow produces higher static charges than a low airflow rate.
c. Some data in this table has been extrapolated.

Static protection measures — computer room environments

Follow these precautions to minimize possible ESD-induced failures in the computer room:

- Maintain recommended humidity level and airflow rates in the computer room.
- Install conductive flooring (conductive adhesive must be used when laying tiles).
- Use conductive wax if waxed floors are necessary.
- Ensure that all equipment and flooring are properly grounded and are at the same ground potential.
- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) and antistatic mats when handling circuit boards.
- Store spare electronic modules in antistatic containers.

Static protection measures — office environments

Office areas generally do not offer the same degree of environmental control possible in a computer room. However, some of the same precautions should be followed:

- Maintain recommended humidity level and airflow rates in the office.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 492
Doc. 3698

- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) and antistatic mats when handling circuit boards.
- Store spare electronic modules in antistatic containers.

Acoustic Safety Standards

The acoustic specifications for the rp24xx server are as follows:

Sound power level	6.4 Bels LWA
Sound pressure level at operator position	58.2 dB LPA

Reducing Acoustic Noise Levels

Ambient noise level in a computer room or office environment can be reduced by the following means:

- Dropped ceiling—Cover with a commercial grade of fire-resistant, acoustic rated, fiberglass ceiling tile.
- Sound deadening—Cover the walls with curtains or other sound deadening material.
- Removable partitions—Foam rubber models reduce noise levels the best.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 493
Doc. 3698

Local Computer Installation Codes

Special local codes exist in some locations regulating the installation of computer equipment. The customer is responsible for making sure their computer system installation is in compliance with all local laws, regulations, and codes for mechanical, building, and electrical distribution systems prior to system installation. The Hewlett-Packard Site Preparation Specialist can assist in determining your local regulations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 494
Doc. 3698

Altitude Operation Standards

Maximum Altitude	
Operational	3000 meters above sea level
Non-operational	4572 meters above sea level

Effects of Altitude

Altitude effects the cooling of computer systems. Less air density means less cooling. Differences in air temperature, input to exhaust, can increase significantly at higher altitudes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 495
Doc. 3698

E C T
CPL - AC

Temperature and Humidity Operation Standards

The following table lists the computer room temperature and humidity specifications for rp24xx servers.

Temperature and Humidity Specifications				
Parameter	**Maximum Non-Operating Range**	**Recommended Operating Range**	**Maximum Operating Range**	**Rate Of Change (per hour)**
Temperature[a]	-40° C to +65° C (-40° F to 149° F)	20° to 25° C (70° to 77° F)	5° C to 39° C (41° F to 102° F)	10° C (50° F) R[b] 20° C (68° F)N[c] 20° F (-7° C)R[b] 30° F (-1° C)N[c]
Operating Humidity	5% to 90%, non-condensing at 25° C (77° F)	40% - 50%, non-condensing at 25° C (77° F)	15% - 80%, non-condensing at 25° C (77° F)	30% RH/hour

a. At altitudes up to 3,000 meters.
b. Repetitive.
c. Non-repetitive.

NOTE Operating ranges refer to the ambient air temperature and humidity measured at the cabinet cooling air intake vents.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 496
Doc. 3698

Electrical Interference Safety Standards

The following are some of the sources of electrical interference that may affect rp24xx servers.

Convenience Wall Outlets

Power outlets for building maintenance equipment (i.e., vacuum cleaners, floor buffers, etc.) must be wired from circuit breakers on a power panel separate from the computer system panel. The ground wires from these outlets must be connected to the normal building distribution panel; not the computer system ground.

If a separate power source and separate ground are not provided, operation of janitorial equipment can induce electrical noise and cause abnormal operation of the computer system. Your electrician can verify whether or not maintenance outlets are on separate panels.

Lightning

In some geographical areas it may by advisable to install lightning protection for both personnel and computer systems. In the United States (USA), the installation of lightning or surge arrestors on power and communication lines is described in the National Electrical Code, Article 280. All lightning arrestors must have the UL 1449 rating and should be tested to survive the suite of IEEE587 tests.

The principles of lightning protection and personnel safety are outlined in detail in the lightning protection code contained in the National Fire Protection Association (NFPA) Handbook.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 497
Doc. 3698

E C T
C P L A C

Other Safety/Operation Standards

The following are some of the other environmental influences that may affect L Class servers.

Vibration

Continuous vibration can cause a slow degradation of mechanical parts and, when severe, can cause data errors in disc drives. Mechanical connections such as printed circuit assembly (PCA) connectors, cable connectors, and processor backplane wiring can also be affected by vibration.

Flammable Materials

Fundamental safeguards for computer systems should include a site well away from any sources of potential damage. The system should not be installed or operated in an environment where there is a risk of fire or explosion due to the existence of highly flammable gases, volatile liquids, or combustible dust.

Airborne Contaminants

Airborne contaminants and particles of a certain size and hardness can damage your computer system, particularly disc drives. Corrosive gases and/or solvent vapors such as those from liquid spirit duplicating equipment and wet-process photo copiers can also cause damage. Some of the most common contaminants are dust, smoke, ash, eraser debris, food crumbs, and salty air.

Electrostatic Discharge

If there is an abnormally high level of static electricity at your computer system's location (15 KV or higher), anyone can cause "sparking" upon contact with the equipment. Carpeting and/or low humidity is a major source of static electricity, especially in dry and cold climates. Static electricity can often be significantly reduced by using a humidifier.

NOTE Hewlett-Packard recommends a heat evaporating-type humidifier and strongly advises against using a cold water atomizer type humidifier

Other ways to minimize electrostatic discharge are by using specially grounded mats in front of the computer system or by treating carpeting with anti-static spray. If spray is used, apply it while the system is turned off. Sprays are very temporary and must be reapplied frequently.

CAUTION Anti-static spray is not recommended because it gets into the system intake filter and coats the circuitry.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 498
Doc. 3698

E C T
I 0320 I
CPL - AC

3 System Site Preparation

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 499
Doc. 3698

ECT - AC

Cooling Requirements

The temperature and humidity specifications shown below are the maximums and standards at which server cooling parameters have been established.

Temperature and Humidity Specifications				
Parameter	**Maximum Non-Operating Range**	**Recommended Operating Range**	**Maximum Operating Range**	**Rate Of Change (per hour)**
Temperature[a]	-40° C to +65° C (-40° F to 149° F)	20° to 25° C (70° to 77° F)	5° C to 35° C (41° F to 95° F)	10° C (50° F) R[b] 20° C (68° F) N[c] 20° F (-7° C) R[b] 30° F (-1° C) N[c]
Operating Humidity	5% to 90%, non-condensing at 25° C (77° F)	40% - 50%, non-condensing at 25° C (77° F)	15% - 80%, non-condensing at 25° C (77° F)	30% RH/hour

a. At altitudes up to 3,000 meters.
b. Repetitive
c. Non-repetitive

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 500
Doc. 3698

ECT - CPL - AC

Input Power Requirements

rp24xx server input power requirements are listed as follows:

Stand Alone Server Power Requirements

- Nominal Rated Voltage: 100 or 240 VAC
- Input Voltage:

  80 to 135 VAC

  176 to 269 VAC
- Input Frequency: 47 to 66 Hz
- Input Current: 1.0 amps at maximum load with input voltage of 88 VAC and 47 Hz

If an Uninterruptible Power Supply (UPS) is to be used, ensure that it is properly connected to the server. Power cord plugs for stand-alone servers are available to meet unique power configurations used all over the world.

Cabinet Mounted Server Power Requirements

Cabinet-mounted servers have the same power requirements as stand-alone servers. However, the power cords for cabinets are dependent on the type of Power Distribution Unit (PDU).

PDU power cords with one end stripped are also available for attaching country-specific power plugs. Refer to cabinet documentation for further cabinet-specific electrical power information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 501
Doc. 3698

Racked Server Site Requirements

rp24xx servers can be configured to operate as a stand-alone server, in a free-standing stack of a maximum of six servers high, or racked in a cabinet. This section provides site requirements for racked server installation.

HP Cabinet Dimensions

Servers can be installed in any of the following HP cabinets:

Cabinet Product Number	Description	EIA	Max. Servers	External Dimensions (width x depth x height)	
				Centimeters	Inches
A4900A	Factory Integrated 1.25m x 19" Cabinet	25	12	59.7 x 100.3 x 125.7	23.5 x 39.5 x 49.5
A4901A	Factory Integrated 1.6m x 19" Cabinet	33	16	59.7 x 100.3 x 161.3	23.5 x 39.5 x 63.5
A4902A	Factory Integrated 2.0m x 19" Cabinet	41	20	59.7 x 100.3 x 196.9	23.5 x 39.5 x 77.5
J1502A	Field Integrated 1.25m x 19" Cabinet	25	12	59.7 x 100.3 x 125.7	23.5 x 39.5 x 49.5
J1501A	Field Integrated 1.6m x 19" Cabinet	33	16	59.7 x 100.3 x 161.3	23.5 x 39.5 x 63.5
J1500A	Field Integrated 2.0m x 19" Cabinet	41	20	59.7 x 100.3 x 196.9	23.5 x 39.5 x 77.5
C2785A	Field Integrated 1.1m x 19" Cabinet	21	10	61 x 91.4 x 111.8	24 x 36 x 44
C2786A	Field Integrated 1.6m x 19" Cabinet	32	16	61 x 91.4 x 162.6	24 x 36 x 64

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 502
Doc.

Stacked Server Site Requirements

rp24xx servers can be configured to operate as a stand-alone server, in a free-standing stack of a maximum of six servers high, or racked in a cabinet. This section provides site requirements for stacked server installation.

NOTE HP will not support stacking of any other A-Class server.

CAUTION In order to remain within weight limitations and to prevent tipping, do not stack servers more than six high. Each server weighs approximately 23 kg (50 lbs). DO NOT lift more than one server at a time.
Always use the strap when stacking servers, regardless of the number. Hewlett-Packard will not support or warrant servers that are damaged as a result of being improperly strapped or stacked more than six servers high.

Server Dimensions

The physical characteristics of the rp24xx server are listed as follows:

Dimension		
Height	9.52 cm	(3.75 in.)
Width	48.26 cm	(19 in.)
Depth	63.5 cm	(25 in.)
Weight	22.68 kg	(50 lbs)

WARNING **DO NOT attempt to lift the server by the front bezel. The plastic bezel is attached by pressing it onto four ball-tipped posts located on the front of the server cover and pulls off with very little pressure.**

The bezel WILL NOT support the 23 kg (50 lb.) weight of the server.

Failure to observe this precaution will cause damage to the server and may cause personal injury.

CAUTION DO NOT stack heavy objects, such as monitors, on top of the server. The weight may cause the top to cave in and damage internal components.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 503
Doc. 3698

ECT - CPL - AC

Stand-Alone Server Site Requirements

rp24xx servers can be configured to operate as a stand-alone server, in a free-standing stack of a maximum of six servers high, or racked in a cabinet. This section provides requirements for stand-alone server installation.

Server Dimensions

The physical characteristics of the rp24xx server are listed as follows:

Dimension		
Height	9.52 cm	(3.75 in.)
Width	48.26 cm	(19 in.)
Depth	63.5 cm	(25 in.)
Weight	22.68 kg	(50 lbs)

Stand-Alone Server Minimum Service Access Requirements

Access Location		
Rear	30 cm	(12 in.)
Left Side	15 cm	(6 in.)
Right Side	30 cm	(12 in.)
Front	30 cm	(12 in.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 504
3698
Doc.

Temperature and Humidity Operation Standards

The following table lists the computer room temperature and humidity specifications for rp24xx servers.

Temperature and Humidity Specifications				
Parameter	**Maximum Non-Operating Range**	**Recommended Operating Range**	**Maximum Operating Range**	**Rate Of Change (per hour)**
Temperature[a]	-40° C to +65° C (-40° F to 149° F)	20° to 25° C (70° to 77° F)	5° C to 35° C (plus or minus 2° C) (41° F to 95° F (plus or minus 3° F))	10° C (50° F) R[b] 20° C (68° F)N[c] 20° F (-7° C)R[b] 30° F (-1° C)N[c]
Operating Humidity	5% to 90%, non-condensing at 25° C (77° F)	40% - 50%, non-condensing at 25° C (77° F)	15% - 80%, non-condensing at 25° C (77° F)	30% RH/hour

a. At altitudes up to 3,000 meters.
b. Repetitive.
c. Non-repetitive.

NOTE Operating ranges refer to the ambient air temperature and humidity measured at the cabinet cooling air intake vents.

4 Server Unpack and Install Instructions

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 506
Doc. 3698

Unpack the Server

Overview

Unpacking the server consists of opening and unloading the carton. Inside the carton you will find, in addition to the server, an accessory kit and a packet containing installation instructions and regulatory information.

NOTE The following instructions do not apply to servers that are received pre-installed in a cabinet. These procedures pertain to individual servers only.

Open and Unload the Carton

Step 1. Place the sealed carton on a work surface with the correct side up as indicated by the, "This Side Up" symbol (shown below).

WARNING **Use sharp instruments carefully when unpacking electronics equipment.**

Failure to follow this precaution may result in personal injury or damage to components.

Step 2. Carefully open the carton, remove the contents, and set them on the work surface. Each carton will contain:

- ❑ The server.
- ❑ A plastic pedestal base for holding the server in a side-mounted position
- ❑ An accessory kit.
- ❑ A packet containing installation instructions and regulatory information.

NOTE Report any missing items to your local Hewlett-Packard office immediately. If there is obvious freight damage, contact your shipper immediately.

We recommend that you retain all packing materials in case any of the items received require return to Hewlett-Packard.

Unpack the Server

WARNING **The rp24xx server weights 22.68 kg (50 lbs). Take necessary precautions to prevent muscle strain when lifting or carrying the server.**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 507
Doc. 3698

Carefully lift the server out of the carton, unwrap it, set it on the work surface.

WARNING **Do not lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency.**
Failure to heed this warning may result in personal injury and/or permanent damage to the server.

Attaching the Pedestal Base

The pedestal base and two accompanying screws included with each stand alone server provides the option of standing the server on its side in order to conserve table space, or standing the server on the floor. To install the pedestal base, follow the instructions listed below:

Step 1. As you are facing the front of the server, carefully stand it on its side with the right side up.

Step 2. Place the pedestal, smooth side down, on the server side and align it lengthwise so that it is parallel with the server.

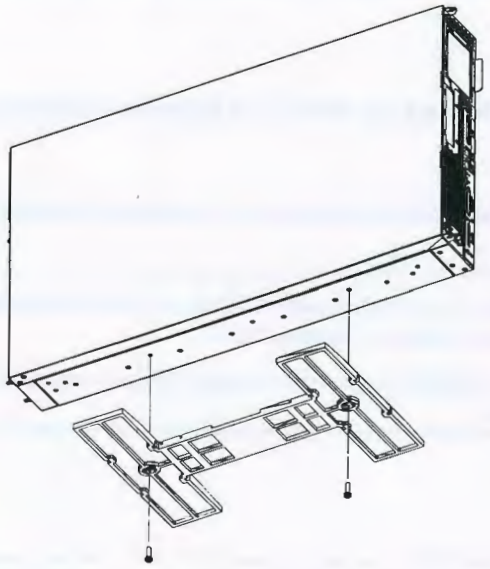
Step 3. Center the pedestal front to rear and align the two recessed oblong holes with the corresponding two holes on the server's side.

Step 4. Insert the two accompanying screws through the bottom of the pedestal and fasten securely to the server.

Step 5. Stand the server on the pedestal.

The following graphic illustrates the pedestal and server.

NOTE The bezel and cover can remain on the server when attaching the pedestal base.



ccrr019

Open the Accessory Kit

Open the Accessory Kit and verify that the contents agree with the packing list.

NOTE Plastic bezel end caps are included in each kit. Do not discard them. They will be needed if the server is installed in a cabinet.

A gray nylon strap is also included. Do not discard it. It will be needed to secure multiple servers (up to six) that are stacked.

Open the Installation Instructions and Regulatory Information Packet

The Installation Instructions/Regulatory Information Packet contains the following information:

- Installation Instruction Sheet, which includes:

  Basic cable connection information necessary to power on and boot the server to the Firmware Main Menu screen.

  The Universal Resource Locator (URL) for the rp24xx server page on the World Wide Web (www.docs.hp.com).

- Compact Disk (CD). Contains the same information available at www.docs.hp.com in the event that access to the Web is unavailable or inconvenient.
- Regulatory Information. Contains consumer safety and regulatory statements for the United States and for those countries that require publishing and dissemination of their own consumer safety and regulatory data.

Third Party Software

NOTE This information is not applicable to e3000 systems.

This server includes licenses for three third-party software products. Please refer to the materials contained in the shipping box for general product information and for instructions on how to download or obtain CDs with this software. The three software products are as follows:

Resonate Central Dispatch

A complimentary three-server license is included. Central Dispatch is an industry-leading enterprise traffic management software solution, ensuring up-time and performance for high traffic, mission-critical e-business applications.

This software package can be found in your accessory box. If you cannot locate the software, or if you require an upgrade to extend the three-server license, please E-mail us at, "mailto:hpsales@Resonate.com". If you need assistance installing Central Dispatch, mail our support team at, "mailto:hpsupport@resonate.com".

You may also register for complimentary Web support for Central Dispatch. Please visit Resonate's website at "http://www.resonate.com/hp"

Infoseek Ultraseek Server

Ultraseek Server is a version of Infoseek's award-winning search technology packaged for use on your intranet or public web servers. It allows users to type question (or just keywords) and instantly find documents relating to the topic on your network.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 508
Doc. 3698

Further product information can be found in your shipping box. If you cannot locate the product information or if you need additional installation assistance, please consult the web site at http://www.ultraseek.com/hp.

Nokia Wireless Application Protocol (WAP) Server

Nokia WAP server is the industry leading WAP server software. It provides seamless functionality with most HTTP servers, retrieving native WML and WML Script content, or converting HTML content to WML.

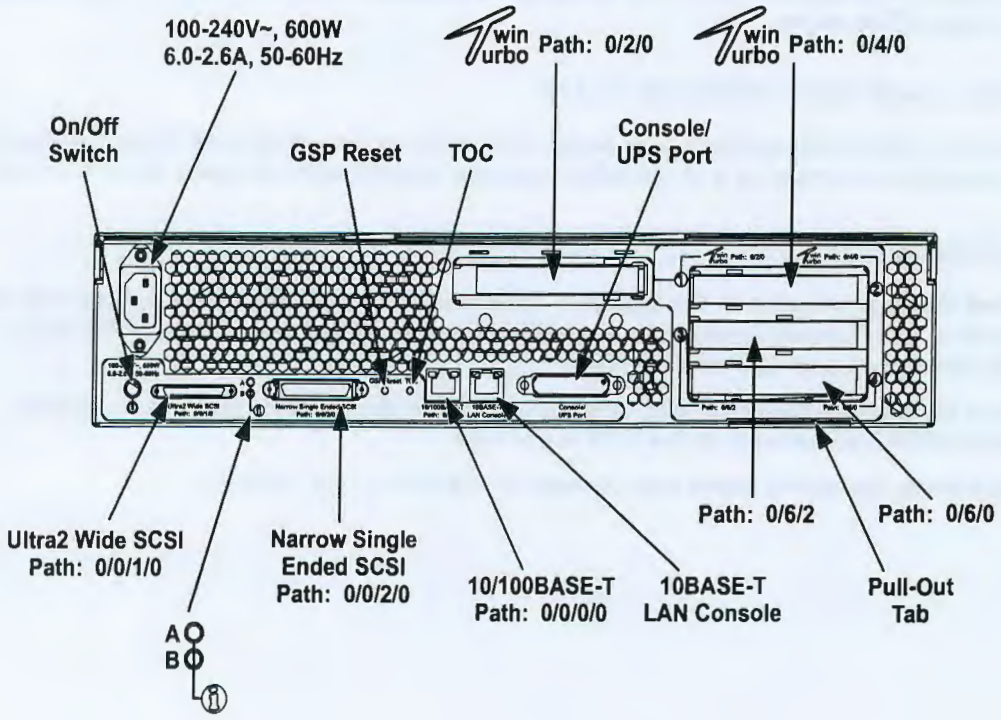
Further product information can be found in your shipping box. If you cannot locate the product information or if you need additional installation assistance, please consult our web site at "http://www.hp.com/go/mobile-aclassoffer".

Server External Connections

External devices are interfaced with the server by means of specific connectors located on the rear bulkhead. Exterior connections to the server include ports for:

- Small Computer System Interface (SCSI) devices
- System Console
- Local Area Network (LAN) Console
- LANs
- Power Cord.

The graphic shown below illustrates locations of the external connections to the server.



ccrr008

Connect External Small Computer System Interface (SCSI) Devices

Connect external SCSI devices to the Single Ended SCSI bus (labeled: *Narrow Single-Ended SCSI Path: 0/0/2/0)* on the system card or to the Ultra 2 SCSI bus (labeled: *Ultra 2 SCSI Path: 0/0/1/0*).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 509
Doc. 3698

Ensure that all devices on the SCSI bus have a unique address and the last device is terminated. Refer to the documentation accompanying each device to learn how to set addresses and where to place terminators.

Connect a System Console

- **Using the ASCII Terminal as a System Console**. If an ASCII terminal is to be used as a console/UPS port, make sure that the keyboard is connected and a power cable is available.
- **Using a SecureWeb Console PCI card as a System Console**. If the Secure Web Console PCI card is to be used as a system console, connect an RJ45 LAN cable to the Secure Web Console PCI card installed in an I/O card slot on the back of the server.

NOTE The Web Console has a default Internet Protocol (IP) address of 192.0.0.192. Make sure that no other device, including other rp24xx servers, has this address before connecting the server to your LAN.

- **Using the LAN Console as a System Console.** If a LAN Console is to be used as a system console, connect it to the system with an RJ45 LAN cable to the RJ45 connector labeled, *10BASE-T LAN Console* connection on the back of the server.

Connect the Core Local Area Network (LAN)

Connect the 10/100BASE-T Core LAN on the system board to the LAN with an RJ45 LAN cable. Connect the RJ45 LAN cable to the server by attaching it to the RJ45 connector labeled, *10/100 Base-T Path: 0/0/0/0.*

Connect Power Cords

Connect the power cord that is provided with the system to the server. For stand-alone servers, the power cord will be localized to each country's power application. If an HP Uninterruptible Power Supply (UPS) is the power source, use the power cord provided with the UPS.

Connect power cords to all external devices at this time with the either the localized power cord, cabinet Power Distribution Unit (PDU) power cord, or the UPS power cord.

For cabinet-mounted servers, the server power cord connects to the PDU in the cabinet.

Installing a Stand-alone Server in a Cabinet

Installing a Stand-alone Server in an HP Cabinet

The following information pertains to rp24xx server installation in cabinets manufactured by Hewlett-Packard only.

Cabinet Identification

The following HP cabinets can hold multiple HP-9000 A-Class, rp24xx servers:

Cabinet Product No.	Assembled by:	Size (Height x Width)	Max. Servers
A4900A	Factory	1.25m x 19"	12
A4901A	Factory	1.6m x 19"	16
A4902A	Factory	2.0m x 19"	20
A5134A (HPe3000)	Factory	1.25m x 19"	12
A5135A (HPe3000)	Factory	1.6m x 19"	16
A5136A (HPe3000)	Factory	2.0m x 19"	20
J1502A	Field	1.25m x 19"	12
J1501A	Field	1.6m x 19"	16
J1500A	Field	2.0m x 19"	20
C2785A	Field	1.1m x 19"	10
C2786A	Field	1.6m x 19"	16
C2787A	Field	2.0m x 19"	20

Cabinet Loading Requirements

Servers require two EIA of cabinet space (each two EIA of space is equivalent to the height of a server). Ensure that the cabinet has this amount of space available.

Fill empty cabinets from the top down. If you are mounting one or more servers into an empty cabinet, start at the inside top of the cabinet and count down four of the holes in the columns at each corner to determine the position of the rails for the first server. When the first rails are installed, continue to use the four hole requirement as your guide for installing additional rp24xx servers.

Installing the Server

The following procedure describes how to install a stand-alone server into an approved cabinet on a slide-rail assembly.

Step 1. Ensure that the anti-tip stabilizers or cabinet ballast are properly installed on the cabinet and secured.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls Nº 510 Dpd 608 07

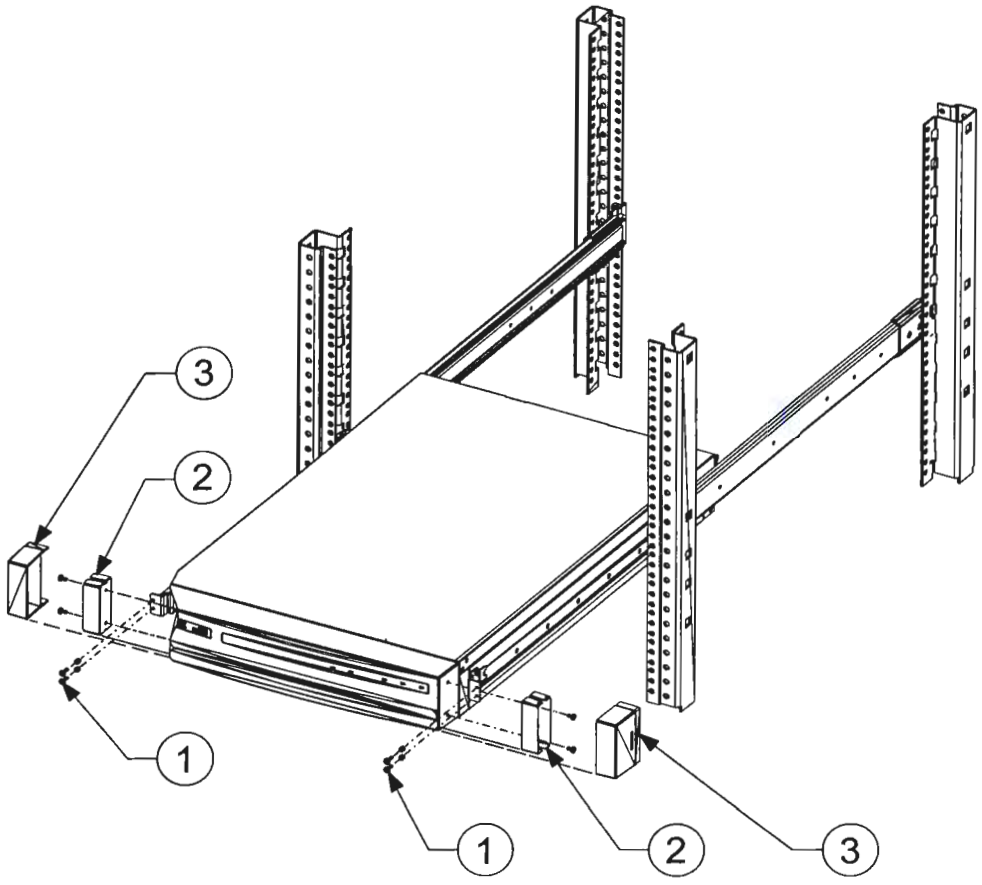
WARNING **If anti-tip stabilizers or ballast are not installed or are improperly installed on the cabinet, it can tip. Failure to follow this precaution can cause personal injury or death and can damage equipment.**

Step 2. Remove the stand alone server from it's packing materials, if not already unpacked.

Step 3. Refer to the *A-400/A-500 Server Slide Rail Installation* instructions, for both server and cabinet rail installation instructions.

Installing Bezel End Caps

Each server is shipped with two metal brackets and two plastic end caps that are designed to be attached to a stand alone server if it is to be mounted in a cabinet. Locate these items and have them available for installation. The following diagram shows the location of bezel end caps and brackets on a racked server.



ccrr001

Callout #	Item
1	Server-to-cabinet attachment screws

Callout #	Item
2	Metal brackets
3	Plastic end caps

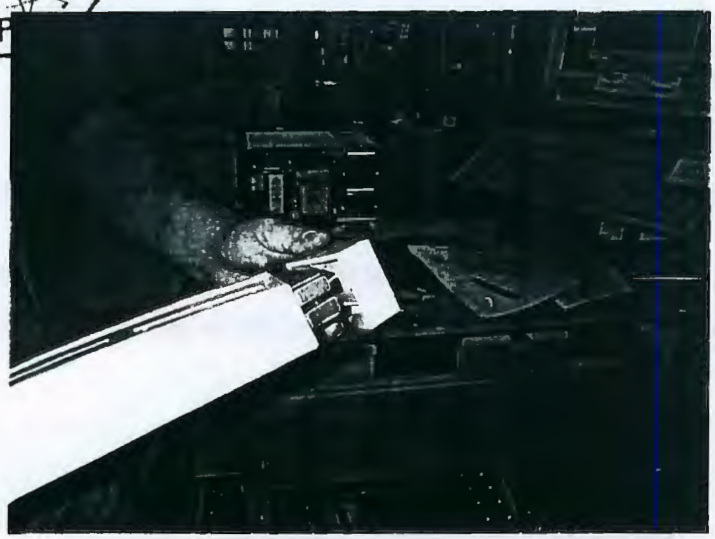
Once the rail kit has been installed and the server is positioned in the cabinet, follow the procedure listed below to attach the brackets and end caps:

Step 1. Extend the server between four and six inches out of the cabinet to allow room to work.

Step 2. Attach the metal brackets to each end of the bezel with two plastic retainers, as shown in the following graphic.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0211
Fls. Nº
Doc: 3698

Step 3. Fit the plastic end caps over the metal brackets as shown below.



Step 4. Push the server back into the cabinet until it is flush against the vertical columns. Replace the screws that fasten the server to the rack.

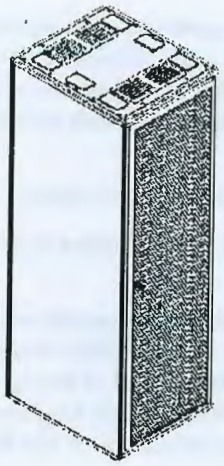
Step 5. Attach the bezel to the front of the server. The cabinet-mounted server will now look like the picture shown below.

Installation In Third-Party Racks

Overview

HP has qualified the rack systems of several vendors as suitable for rp24xx server installation.

To qualify each rack configuration, specific rack vendors and rack products have been identified. Each vendor has several rack product lines. rp24xx servers are supported only in HP cabinets or in qualified vendor racks, as shown below:



Examples of cabinets are Chatsworth (CPI) Megaframe, Wrightline Paramount, Rittal Vario, Vero IMRAK, SMC, Zero Express Rack and Bud Industries S2000. For further information, refer to the table titled, *Third Party Rack Ordering Guide for Vendor Products*, at the end of this section.

Third Party Rack Checklist for rp24xx Server Installations

This document is a guide to insure safe and reliable installation and operation of rp24xx servers in third party EIA-style racks and applies to installations at the end-customer site only.

Footprint

The rp24xx server is 25 inches deep. Additional space for cable management is required in the rear. HP recommends 40 inches in front and 24 inches in the rear for service access and proper safety in proximity to energized electronic equipment.

Safety Checklist

To insure the installation is safe, the following items must be addressed:

Anti-tip safety	The rp24xx server slides out of the rack about 24 inches for service. When extended this far, there can be a major tip hazard for the rack. If the rack has anti-tip feet front and rear, attach them prior to installing the server. If anti-tip feet are not available, ensure that the rack is solidly bolted to the floor both front and rear. Ensure that the thick sheet metal of the rack base provides for a bolt-down bracket.
Rack slides	When servicing the HP rp24xx server, it is critical to use properly attached rack slides, which will allow the detents to stop the sliding motion of the unit. Always work on the server when it is fully extended and locked in place to avoid injury to maintenance personnel.

Warranty Checklist

The following factors must be considered to insure that HP's warranty is valid in third party rack configurations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 512
Doc. 3698

Air flow

rp24xx servers require front-to-back airflow. Therefore, a solid front or rear door will not work. The doors must be removed or changed to a 63% open perforation pattern over an area 17 inches wide, top to bottom, minus a 2 inch border. Also insure that the hot air exhaust from other equipment is not being presented to the intake (front) of the rp24xx server.

Service Access

To insure that the rp24xx server can be serviced properly, the installation must allow for a free sliding distance of 40 inches out the front of the rack. This will also allow HP to use the standard service contract for any rp24xx server in the field regardless of the racking situation. Alternate service contracts are addressed later in this document.

Cable strain relief

The cable management solution for the rp24xx server is in two parts:

1. There is a wire-form cable management system that attaches to the rear of the server that provides a strain relief attachment point.
2. The cable bundle from each server must be Velcro tie-wrapped and fed into a 40 inch service loop. The service loop allows the server to slide forward completely out of the rack for access. For warranty purposes, a proper method of strain relief must be used, especially for any SCSI-type cables on the PCI cards. This may force the elimination of the rear door in some cases. Judgement is required based on the following examples:

- MINIMAL CABLING- If the customer has a power cable and two LAN cables attached to the rp24xx server, cabling options include an alternate strain relief system, to allow the rear door (if perforated) to be used for security.
- FIBER OPTICS CABLING – Fiber optics cable allows a 1.5 inch bend radius and has a very low profile connector. Fiber optics cable bundles are relatively small and can be held to the inside of the wire-form strain relief.
- MAXIMUM SCSI CABLING – If ultra-flex SCSI cables are used, the bend radius allowable is 1.5 inches with a low profile connector. the customer must use the provided wire form strain relief parts. HP strongly recommends using a server rack that provides the extra space required to house excess cabling.

rp24xx server PDU Support

PDUs for rp24xx servers must be ordered as separate products when configuring a Third Party Rack order.

The PDUs are:

Table 0-2

E7674A 19"	16A	100-240V
E7681A 19"	30A	100-240V
E7682A 19"	60A	100-240V

Supportability Matrix

The following table shows supportability requirements.

Table 0-3

Major Features	rp24xx server w/ Full HA

Table 0-3 (Continued)

Anti-Tip	MUST
Proper slides	MUST
Airflow	MUST
Service Access	MUST
Cable Strain Relief	MUST
Front Access	40 inches
Rear Access	24 inches

Third Party Rack Ordering Guide for Vendor Products

Table 0-4

Rack	Mounting Hardware	Doors	Qualified Tip Stability Device	Contact
Chatsworth Megaframe Rack (cabinet)	12468 Series Full Rack Mounting Rail, pair[a] 12464 Series Half Rack Mounting Rail, pair[a]	14032 Series Perforated Metal Door	712441-001 Floor Clamp Kit	www.chatsworth.com

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 513
Doc. 3698

Table 0-4 (Continued)

Rack	Mounting Hardware	Doors	Qualified Tip Stability Device	Contact
Wrightline Paramount Frame 40" Deep JF842440	JRK44190 Rail Kit and JHP0N001 rp24xx server Adaptor Bracket	JDF8242L Paramount 84" x 24" left-hinged JDF8424R Paramount 84" x 24" right-hinged JDP84242 Paramount Frame perforated door insert for 84" x 24" door frame JTPP2440 perforated top panel - 24"W x 40"D	Floor anchoring	www.wrightline.com
SMC 36" Deep LAN Storage Module	rp24xx server Adaptor	Ventilated Front and Rear	Floor anchoring	Sales & Customer Support 1-800-SMC-PLUS (1-800-762-7587)

a. Requires purchase of two.

NOTE For additional or other third party rack vendor product information, contact the HP Enclosures Technical Marketing Manager at (408) 873-6692.

Server Slide Rail Installation

The following information contains instructions for installing rp24xx servers in a cabinet.

CAUTION Both anti-tip feet must be properly affixed before installing equipment in a cabinet on a slide assembly.

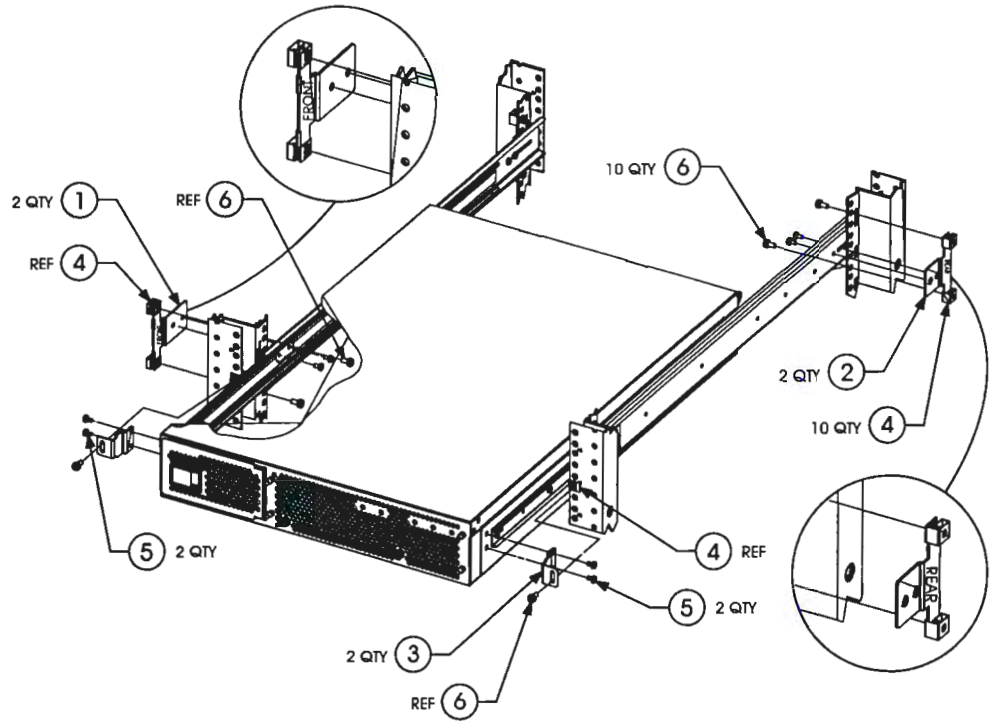
Tools needed: Torx Drivers, T15 and T20.

Slide Rail installation kit contents are as follows:

2	Slides, inner
2	Slides, outer
2	Slides mount, front
2	Slides mount, rear
2	Plastic bezel end caps
1	Cable Management device
1	see-through plastic bag containing: 2 bracket end caps 2 rack mounting ears
1	see-through plastic bag containing: 2 front RBI adapters 2 rear RBI adapters 2 cres fr flanges 4 M4 x 0.7 screws 10 10/32 x 0.5" screws 10 Sheet metal nuts (Note: Contains non-E-series HP cabinet hardware, also)
1	see-through plastic bag containing: 4 plastic snap rivets 4 sheet metal nuts 8 M5 screws 16 M4 screws

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 514
3698
Doc.

The following illustration shows rail parts only. Plastic parts bags, plastic end caps, and the cable management device is not shown:



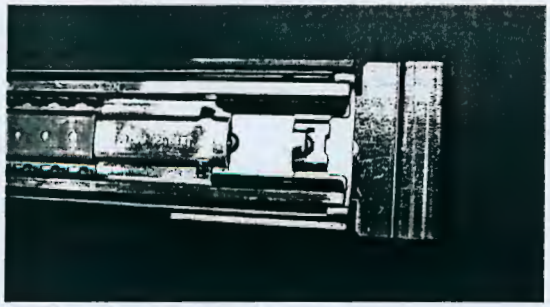
RACK KIT ASSEMBLY

ITEM	QTY	PART/MATERIAL-DESCRIPTION	PART NUMBER
6	10	SCREW, 10-32 x 0.5 INCH	2680-0278
5	4	SCREW, M4 x 0.7mm	0515-2478
4	10	SHEET METAL NUT	0590-0804
3	2	FLANGE	A5570-00044
2	2	ADAPTER, REAR	A5570-00043
1	2	ADAPTER, FRONT	A5570-00042

NOTE This illustration shows non-E-series HP cabinet columns

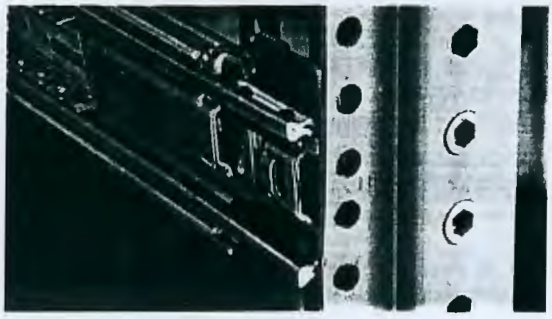
The following procedures list the steps required to install a stand-alone server in a cabinet.

Step 1. Attach rear slide mounts to the outer rails using M4 x 0.7mm screws. Do not fully tighten screws. Allow the rear slide mount to move along slot in the outer rail.



Step 2. Place the outer rails with mounting brackets in the rack. Engage support hooks in the rack columns. The front mounts and rear mounts are different, as shown below:

Support Hook attached to rack column.

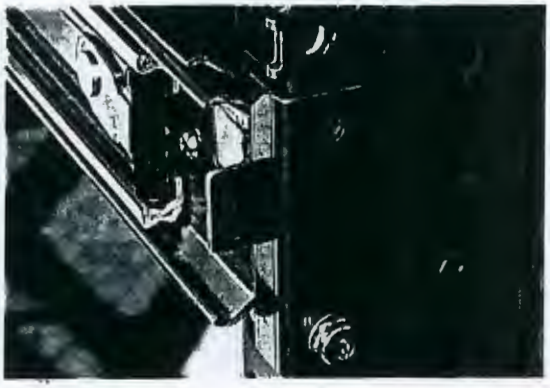


Front Slide Mount Placement

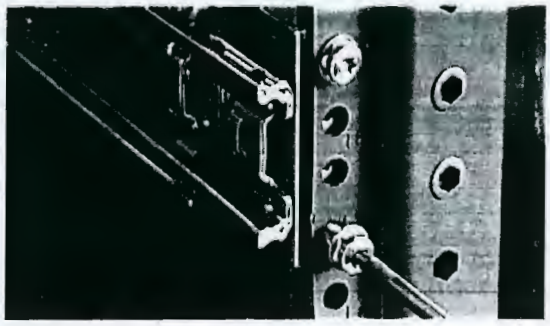
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 515
Doc. 3698

Rear Slide Mount Placement

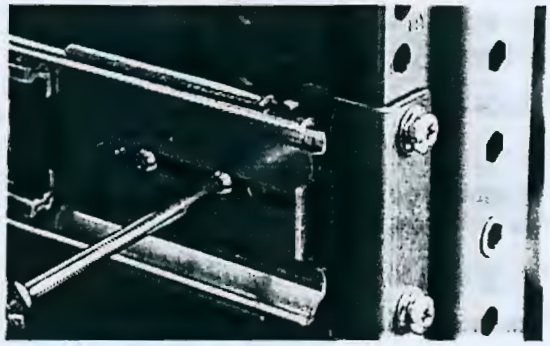
Step 3. Install sheet metal nuts on rear columns. Locate the slide mount laterally against rack column. Install and tighten the M5 x 0.8mm machine screws.



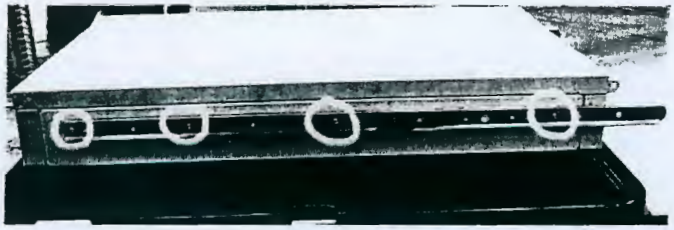
Step 4. Install and tighten the M5 x 0.8mm machine screws on the front slide mounts.



Step 5. Tighten the M4 x 0.7mm screws that attach the slide rails to the rear mounts.



Step 6. Locate and install the inner slides on the sides of the server, using M4 x 0.7mm machine screws. The inner rails contain a flat spring latch. The free end of the latch goes toward the front of the server, the riveted end goes toward the rear of the server chassis.



Step 7. Double-check all mounting screws to ensure that they are tight.

Step 8. Completely extend both outer slides to the front of the rack. Outer slides should latch in the extended position.

Step 9. Align the inner rails on the server between the extended outer rails on the rack.

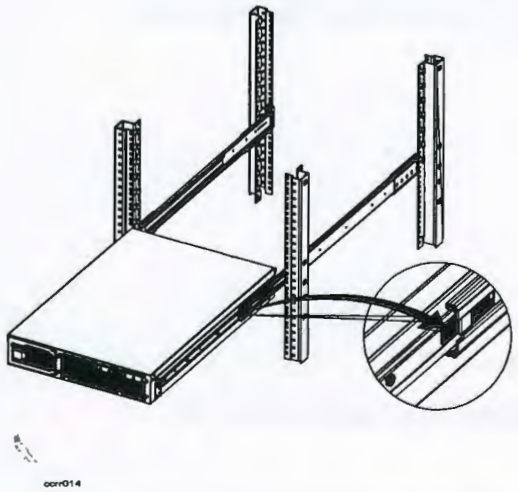
WARNING **The rp24xx server weights 22.68 kg (50 lbs). Use two people or a lift during installation. Take necessary precautions to prevent muscle strain when lifting or carrying the server.**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 516
Doc.

Do not lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency. Failure to heed this warning may result in personal injury and/or permanent damage to the server

NOTE The rail sets on both sides of the chassis must be properly aligned and engaged before attempting to slide the server into the cabinet.

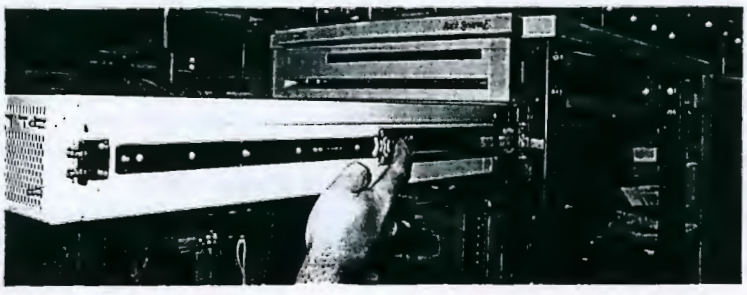
The inner rail (attached to the server) must have *both* top and bottom edges *inside* the outer (cabinet) rails



Step 10. Carefully guide the inner slide rails on the server chassis into the outer rails, engaging the ball bearing carriers.

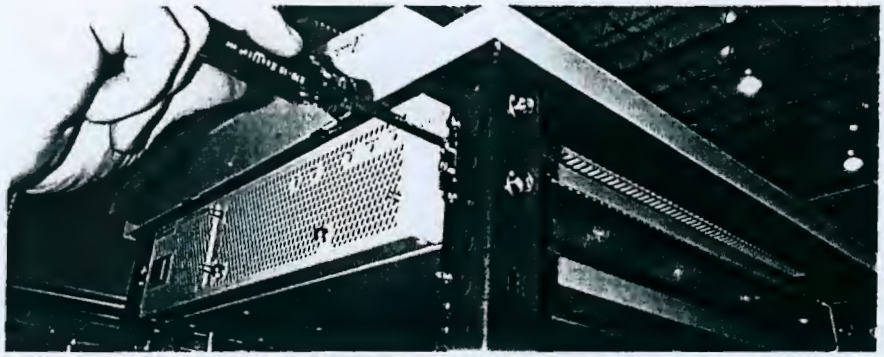
CAUTION Do NOT force the slides together. To do so may damage the ball bearing carriers. The inner slides will latch after travelling a few inches.

Step 11. Press the slide latches on the inner slides and carefully slide the server completely into the rack.

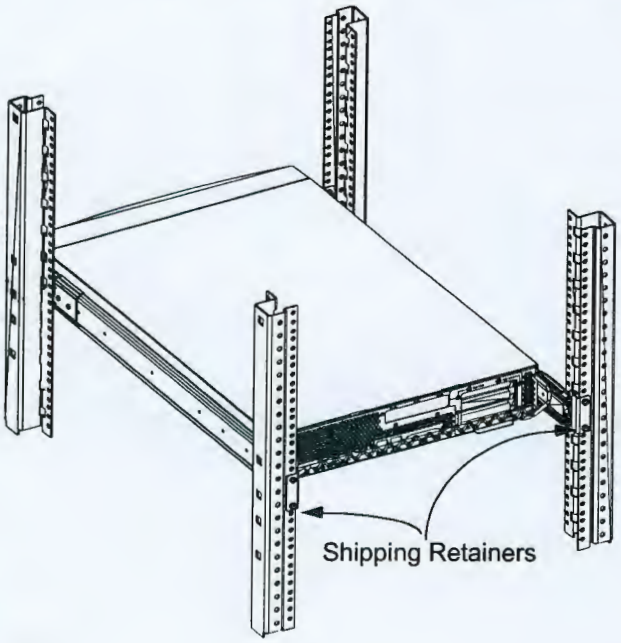


Step 12. Verify operation of the slides and check alignment of the server in the rack.

Step 13. Secure the server to the rack columns with M4 x 0.7mm screws and M4 clip nuts.



Step 14. Optional: Install shipping retainers at the rear of the unit if the server is to be shipped while installed in a rack. Install retainers with M5 x 0.8mm screws and M5 clip nuts.



ccm013

RQS nº 03/2005 - CN
CPMI - CORREIOS
517
Fls. Nº
3008
Doc.

Cabinet Installation

Cabinet Installation

Installation of a factory-loaded cabinet consists of the following steps:

Step 1. Move the cabinet to the installation site.

Step 2. Lower the leveling feet. (This will prevent excessive wear on the casters, level the cabinet, and provide stability.)

WARNING **Extend or install the cabinet stabilizers, located at the bottom of the front of the cabinet, as an additional safeguard against the cabinet toppling forward during installation.**

Failure to observe this precaution could result in personal injury or death and equipment damage.

Step 3. Connect the console and system peripherals to the server(s).

NOTE Attaching cables while the rails are extended fully forward will ensure that sufficient slack is available for later maintenance.

Step 4. Connect the cabinet power cord to the appropriate wall outlet.

Step 5. Be sure all peripherals outside the cabinet are connected to wall outlets.

The cabinet/server system assembly is now ready for the power up process.

RQS nº 03/2005 - CN
CPMI - CORREIOS
518
Fls Nº
Doc. 3698

Cabinet Mounted Server Unpack

Overview

rp24xx servers can be procured in two modes: stand-alone or pre-installed in a cabinet at the Hewlett-Packard factory. Stand-alone servers can be installed in an existing HP-supported cabinet by purchasing Rail Kit A5810A.

Installing a Factory-integrated Cabinet

Unpacking the Cabinet

NOTE It is the customer's responsibility to inspect the shipping package for damage.

It is the Hewlett-Packard Customer Engineer's responsibility to remove the cabinet assembly from the shipping pallet.

WARNING **A fully configured 2.0 meter cabinet can weigh over 500 kg (1100 lbs). Be careful not to tip the cabinet while unpacking.**

Failure to heed this warning can result in serious injury or death and equipment damage.

To unpack the cabinet, perform the following steps:

WARNING **Wear protective glasses while cutting the plastic bands around the shipping container. These bands are under tension.**

Failure to heed this warning can result in serious eye injury if the severed bands snap back and hit you in the face.

Step 1. Cut the plastic polystrap bands around the shipping container.

Step 2. Follow the procedure listed below to prepare the cabinet for removal from the pallet:

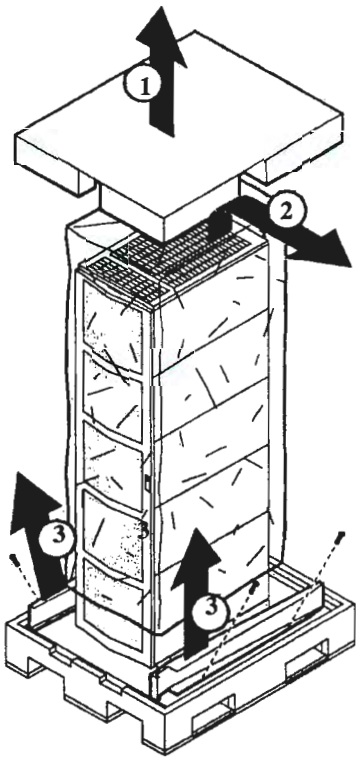
a. Lift the cardboard top cap off of the shipping box (callout 1).

b. Remove the packing material underneath the cap (callout 2).

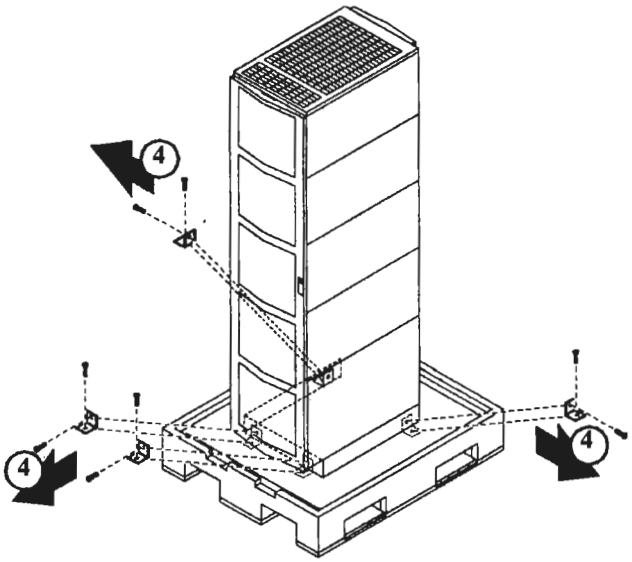
c. Remove the clamshell box and place out of the way.

d. Remove the screws that secure the ramps in place and lift the ramps out (callout 3).

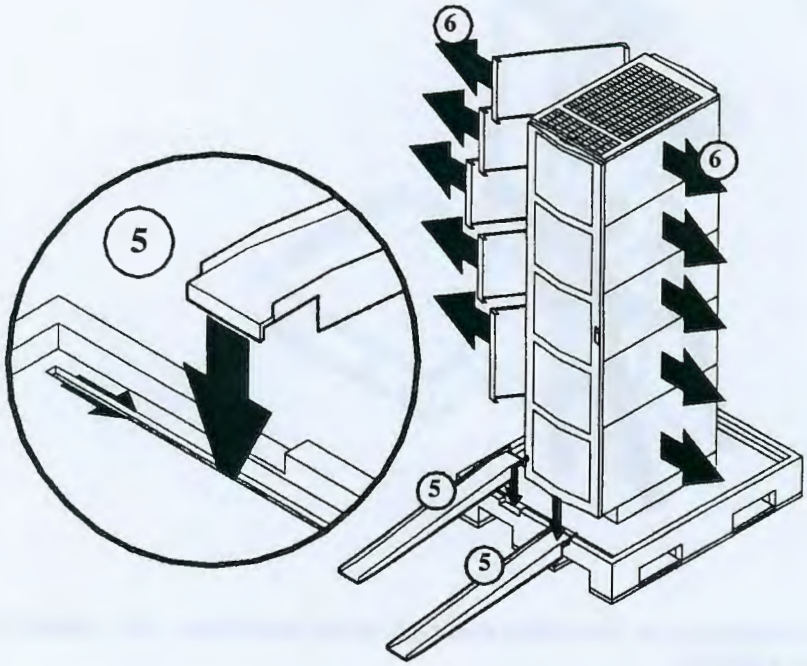
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 519
Doc. 3698



Step 3. Remove the brackets securing the cabinet to the pallet (callout 4).



Step 4. Insert the ramps in the notches provided on the pallet (callout 5). Remove the side panels from the cabinet and set them aside (callout 6).

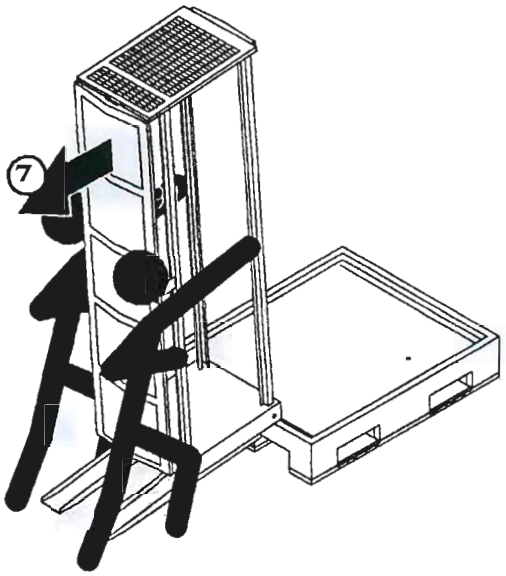


WARNING: A fully configured 2.0 meter cabinet can weigh over 500 kg (1100 lbs). Always use at least two people to roll the cabinet off of the pallet. Be careful not to tip the cabinet while unloading.

Failure to heed this warning can result in serious injury or death and equipment damage.

Step 5. Use at least two people to roll the cabinet off of the pallet and down the ramp (callout 7).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 520
Doc. 3698



Cabinet Inspection

Once the cabinet is off the shipping pallet, but before moving it to the installation site, inspect the internal and external condition of the cabinet.

Cabinet Exterior Checklist

Check the cabinet exterior for signs of shipping damage:

- ❑ Look at the top and sides for dents, warpage, or scratches.
- ❑ Check the server front bezels for alignment, scratches and breakage.
- ❑ Check any filler panels on the front of the cabinet for proper fit.
- ❑ Check the rear door for dents, scratches, proper fit when closed, and operation.

Cabinet Interior Checklist

Open the rear door and inspect the inside of the cabinet:

- ❑ Inspect all cables and ensure that they are secure.
- ❑ Inspect all rails for signs of damage.
- ❑ Check all mounting screws for tightness.
- ❑ Check all components for signs of shifting during shipment or any signs of damage.

NOTE If the shipment is either incomplete, damaged, or fails to meet specifications, notify the nearest Hewlett-Packard Sales and Support Office. If damage occurred in transit, notify the carrier as well. Hewlett-Packard will arrange for replacement or repair without waiting for settlement of claims against the carrier. If the shipment was damaged in transit, keep the shipping containers and packaging material for inspection. If extensive damage is found, it may be necessary to return the entire cabinet to HP.

PowerTrust Uninterruptible Power Supply (UPS) Option

Unpack the PowerTrust UPS and use the installation information in the *PowerTrust System Guide,* included with the UPS, to connect the UPS to the cabinet.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 521
3698
Doc.

Repackaging the Cabinet for Shipment

Use the original packing material to repackage the cabinet for shipment. If the packing material is not available, contact your local Hewlett-Packard Sales and Support Office regarding shipment.

Before shipment, place a tag on the container (or equipment) to identify the owner and the service to be performed. Include the equipment model number and the full serial number, if applicable. The label showing the model number and the full serial number is located on the outside of the rear door.

Due to the weight of a fully loaded cabinet, it will require two people to push the cabinet up the ramp onto the pallet.

WARNING: Repackaging a loaded cabinet may be hazardous because a fully configured 2.0 meter cabinet can weigh up to 500 kg (1100 lbs). Always use two people when moving the cabinet and when positioning the cabinet on the pallet. Check the condition of the loading/unloading ramp before use. If the ramp appears damaged, DO NOT attempt to push a loaded cabinet up the ramp onto the pallet. Contact your local Hewlett-Packard Sales and Support Office regarding shipment. Failure to heed this warning can result in serious injury or death and equipment damage.

To repackage the cabinet, follow the repacking checklist and refer to the unpacking instructions for detail.

Repacking Checklist:

- ❑ Assemble the HP packing materials that came with the cabinet.
- ❑ Connect the loading ramp to the pallet.
- ❑ Raise the cabinet levelers before moving the cabinet.
- ❑ Retract or remove the stabilizers.
- ❑ Push the cabinet up the ramp onto the pallet. Be sure to position the cabinet so that the front goes up the ramp first.
- ❑ Secure the cabinet to the pallet with the shipping clamps, shipping block, and rear door support.
- ❑ Place the anti-static bag over the cabinet.
- ❑ Place bezel support packing on the front corners of the cabinet. Secure it with a wrap.
- ❑ Place the top cap packing material and loading/unloading ramp on top of the cabinet.
- ❑ Wrap the clam shell box around the cabinet.
- ❑ Put the box top on the box and secure the assembly to the pallet.

Be sure to follow the tagging and labeling instructions mentioned earlier. The cabinet is now ready for shipment.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 522
Doc.

Stacking Servers

Hewlett-Packard will support stacking up to six rp24xx servers if the following conditions are met and the correct procedure followed.

NOTE HP will not support the stacking any other A-Class server.

CAUTION In order to remain within weight limitations and to prevent tipping, do not stack servers more than six high. Each server weighs approximately 23 kg (50 lbs). DO NOT lift more than one server at a time.
Always use the strap when stacking servers, regardless of the number. Hewlett-Packard will not support or warrant servers that are damaged as a result of being improperly strapped or stacked more than six servers high.

Follow the steps listed below:

Step 1. Remove the rubber "feet" from the packing material and place one rubber foot squarely on each of the four corners on the bottom of each server.

Step 2. Lay the enclosed binding strap out flat and straight.

WARNING **DO NOT attempt to lift the server by the front bezel. The plastic bezel is attached by pressing it onto four ball-tipped posts located on the front of the server cover and pulls off with very little pressure.**

The bezel WILL NOT support the 23 kg (50 lb.) weight of the server.

Failure to observe this precaution will cause damage to the server and may cause personal injury.

Step 3. Place the first server over the strap and position the strap so that it can be firmly cinched down on the top server.

Step 4. Carefully set the remaining servers (up to five) on top of the first server so that the four feet of each of the remaining servers are squarely on the top of the server below.

WARNING **Do not cinch the strap so tightly that the chassis buckles.**

Failure to heed this precaution may cause internal components to be damaged and/or the server cover may not seat correctly to seal the server from dirt and dust.

Step 5. Center the strap midway between the front and rear of the stack and pull the ends up over the top server. Thread the flat end through the loop end and pull it snug. Press the Velcro® pieces together firmly and lay them flat on the top cover of the top server.

RQS nº 03/2005 -107
CPMI - CORREIOS
Fls. Nº 523
Doc. 3698

CAUTION DO NOT stack heavy objects, such as monitors, on top of the server. The weight may cause the top to cave in and damage internal components.

Unstacking Servers

If internal access (for maintenance or component removal and replacement, etc.) is required to a stacked server (with the possible exception of the top server), the stack must be unstrapped and the servers unstacked to remove the cover of the unit for which internal access is required (target server).

NOTE HP will not support the stacking of any other A-Class server.

CAUTION In order to remain within weight limitations and to prevent tipping, do not stack servers more than six high. Each server weighs approximately 23 kg (50 lbs). DO NOT lift more than one server at a time.
Always use the strap when stacking servers, regardless of the number. Hewlett-Packard will not support or warrant servers that are damaged as a result of being improperly strapped or stacked more than six servers high.

Follow the steps listed below:

Step 1. Pull the flat end of the strap out of the loop end and pull the Velcro® pieces apart.

WARNING **DO NOT attempt to lift the server by the front bezel. The plastic bezel is attached by pressing it onto four ball-tipped posts located on the front of the server cover and pulls off with very little pressure.**

The bezel WILL NOT support the 23 kg (50 lb) weight of the server.

Failure to observe this precaution will cause damage to the server and may cause personal injury.

Step 2. Carefully remove the servers in the stack, one at a time, until the target server is reached.

TIP At this point, a decision to remove the target server or leave it in place to work on it can be made. Removing the target server will allow you to restack the remaining servers and continue using them while the target server is being repaired.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 524
Doc. 3698

5 Operating Instructions

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 525
Doc. 3698

Configuring the Guardian Service Processor (GSP)

The Guardian Service Processor (GSP) is resident in the system to allow the system administrator to monitor and perform administrative functions locally on the system console, or at a console in another area. This section provides configuration procedures that will:

- Configure the GSP Local Area Network (LAN) port
- Add or delete GSP users (maximum of 20)
- Change the default GSP configuration.

Configuring the GSP LAN Port

Perform LAN configuration from the system's local port (either console or the HP secure web console).

NOTE The GSP LAN port is different from the System LAN. It will need a separate:

- 10BaseT LAN connection
- Subnet mask
- Gateway address
- Hostname (to be used when messages from the console are logged or printed)

To configure the GSP LAN port, perform the following steps:

Step 1. To select the GSP, enter: **ctrl + b**.

Step 2. At the GSP prompt, enter the following LAN Configuration (lc) command:

```
GSP> lc
```

The *lc* comrp24xxmand will start a series of prompts. Respond to each prompt with the appropriate information.

Adding Users

The GSP stores access information for a maximum of 20 users (one administrator and 19 operators). By design, the first user entered into the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users, or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

To add a user, perform the following steps:

Step 1. Type **ctrl + b** to access the GSP.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 526
Doc. 3698

Step 2. At the GSP prompt, enter the Security options and access control (SO) command:

```
GSP> so
```

Step 3. The first prompt you will see with the *so* command is for the following GSP-wide parameters:

- Login Timeout: 1 minutes.
- Number of password Faults allowed: 3.
- Flow Control Timeout: 5 minutes.

The terminal will then display:

```
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

Enter **Y** to modify GSP-wide parameters, or enter **N** to continue to add users.

If you enter Y, the parameters will be displayed in an edit mode to allow modification.

If you enter N, continue to the next step.

NOTE The first user entered (user number 1) is identified as the GSP administrator.

If you are adding users, you will need to step through all current user entries to reach the next available user prompt.

Step 4. The terminal will display:

```
Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __
```

Enter **Y** to modify user number 1 parameters, enter **N** to leave user number 1 parameters unchanged or enter **Q** to quit and return to the GSP prompt.

If you enter Y, the parameters will be displayed in an edit mode to allow modification.

If you enter N, the terminal will display:

```
Do you want to modify the user number 2 parameters? (Y/[N]/Q to quit) __
```

Enter Y, N, or Q and proceed according to the instructions shown above in this step.

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry could deny entry to that user.

The following list is an example of added users information:

User's Name: Joe Smith
Organization's Name: IT Support
Dial-back configuration: Disabled
Access Level: Operator
Mode: multiple
User's state: enabled

For the number 1 user, the Access level is administrator.
A Mode entry of single only allows entry for that user one time, after which, further logon attempts are denied and the user state is set to disabled.
A Mode entry of multiple allows unlimited logon access to the GSP for that user.

Removing Users

You can remove (disable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

Step 1. Enter **ctrl + b** to access the GSP.

Step 2. At the GSP prompt, enter the Security options and access control (SO) command:

```
GSP> so
```

Step 3. The first prompt you will see with the *so* command is for the following GSP-wide parameters:

- Login Timeout: 1 minute.
- Number of password Faults allowed: 3.
- Flow Control Timeout: 5 minutes.

The terminal will then display:

```
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

Enter N and continue to the next step.

NOTE You may need to step through several user numbers until you reach the user to be removed.

Step 4. When you access the number of the user to be removed, modify the User's state to *Disabled* and change any other user information necessary.

Changing the Default GSP Configuration

This section describes the process of changing GSP default configuration to the default (factory preset) values. To reset the GSP to its default configuration, perform the following steps:

Step 1. Enter **ctrl + b** to access the GSP.

Step 2. At the GSP prompt, enter the Default Configuration (dc) command:

```
GSP>co
```

Step 3. Follow the prompts to change all GSP configurations to the default values.

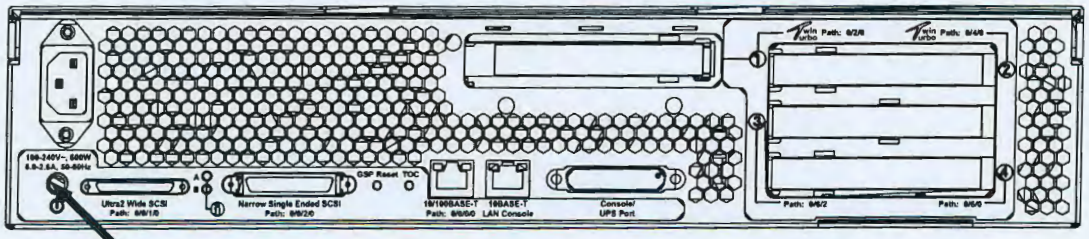
CAUTION When the Security configuration is reset using the *GSP>dc* command, all users, including the GSP administrator, are removed *Remote* is disabled, and the network configurations are reset to the factory default values. The *Remote* functionality must be re-enabled through the main console using the Enable Remote (er) command. The IP address, hostname, subnetmask, and the gateway IP must be re-entered through the main console using the *LAN Configuration* (lc) command.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 527
3698
Doc.

Initial Power-up

The following section describes the process of applying power to the server and booting the system to the operating system Login prompt.

1. Apply AC Power to the system console.
2. Apply power to the server by pressing the rear panel On/Off switch IN.



ccrr012

3. A series of self-test boot progress messages will scroll rapidly up the screen. Some messages may pause for up to one minute while the test completes.
4. The initial power-up selftest process will complete in one to five minutes and the Boot Console Handler (BCH) main menu will be displayed.
5. To start the boot process using the primary boot path, type *BO PRI*, at the BCH main menu prompt and press **ENTER**.

NOTE Booting a system to a operating system login prompt from BCH main menu can take 20 minutes or longer depending on your software and hardware configuration.

6. Once the system reaches the operating system login prompt, a display similar to the following will be shown on the console screen:

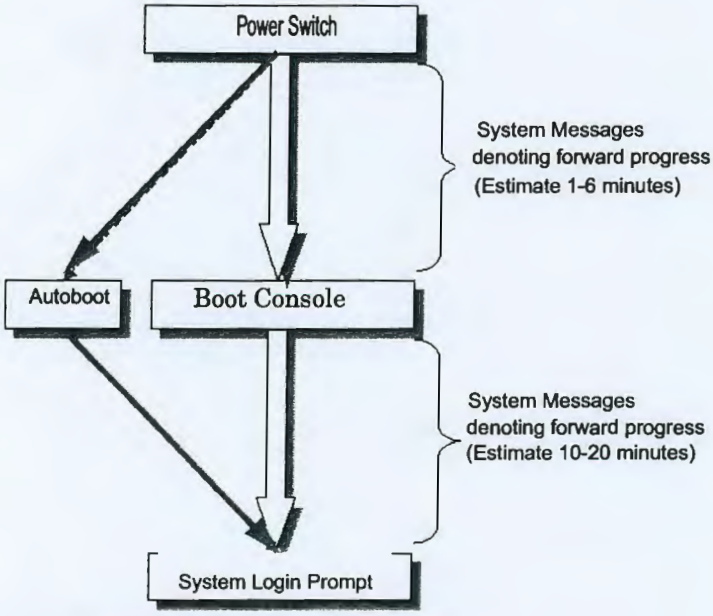
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 528
Doc. 3698

Boot To Operating System

The length of time required to boot the system depends on the number of processors and the amount of RAM memory installed. Average configurations can take 20 minutes or more.

The boot process is shown in the following illustration:

Typical Boot Process



The duration of the full boot process can vary depending on:

- Number of CPUs installed
- Amount of Memory installed
- Operating System version installed
- State of the network

(Total time to boot will vary)

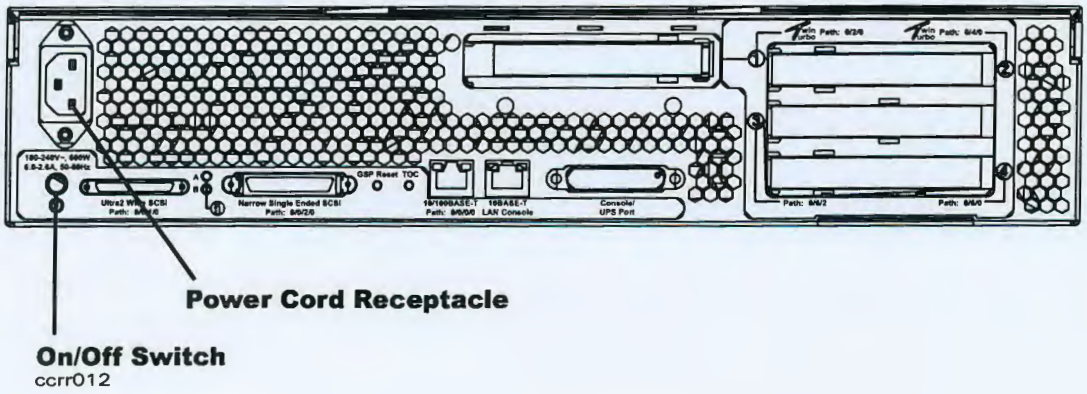
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 529
Doc.

System Power Down

1. Stop all active applications that may be running and Log Off all users.
2. Perform a system backup of the entire Operating System and data base. If this is not feasible, perform a backup of the data base. (Backups should be performed at a scheduled interval as common practice for protecting any new data or changes to the existing data base.)
3. To shut down the OS, enter, "`/etc/shutdown -h`" at the prompt.
4. At the rear of the computer, press and release the on/off switch to power-down the server.

NOTE Housekeeping voltage is still present after switching power off. Unplug the power cord to completely remove power.

5. Unplug the power cord from the server.



ccrr012

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 530
Doc.

E C T
I CPL - AC I

6 Adding Components to the Server

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 531
Doc. 3698

Add Memory

Memory Configuration Rules

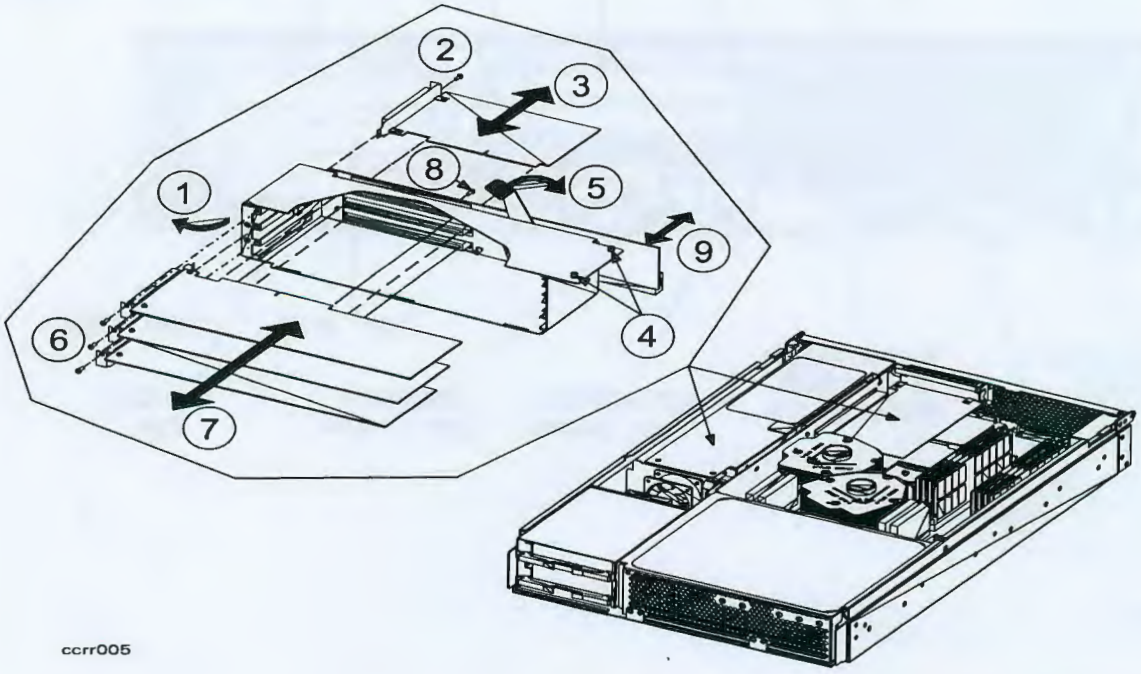
rp24xx servers have 8 slots (4 DIMM pairs) on the system board for memory DIMMs. These slots are numbered 1through 8. Four slots (5 - 8) are disabled on A400 servers. A500 servers can access all slots. The following rules govern the installation of memory DIMMs:

- Memory must be installed in DIMM pairs.
- The capacity of DIMMs within a pair must be the same.
- Install DIMMs with the greatest capacity in the lowest slot numbers.
- Install DIMMs in numerical order starting with slot 1 (1, 2, 3, etc.).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 532
3698
Doc.

Add Peripheral Component Interconnect (PCI) Cards

rp24xx servers have a total of 4 PCI I/O slots. Slot 1 is short slot, located outside the I/O card cage, connected to the back of the I/O Backplane. Slots 2 through 4 are located inside the I/O card cage. Slots 1 and 2 are Twin Turbo slots; slots 3 and 4 are Turbo slots.



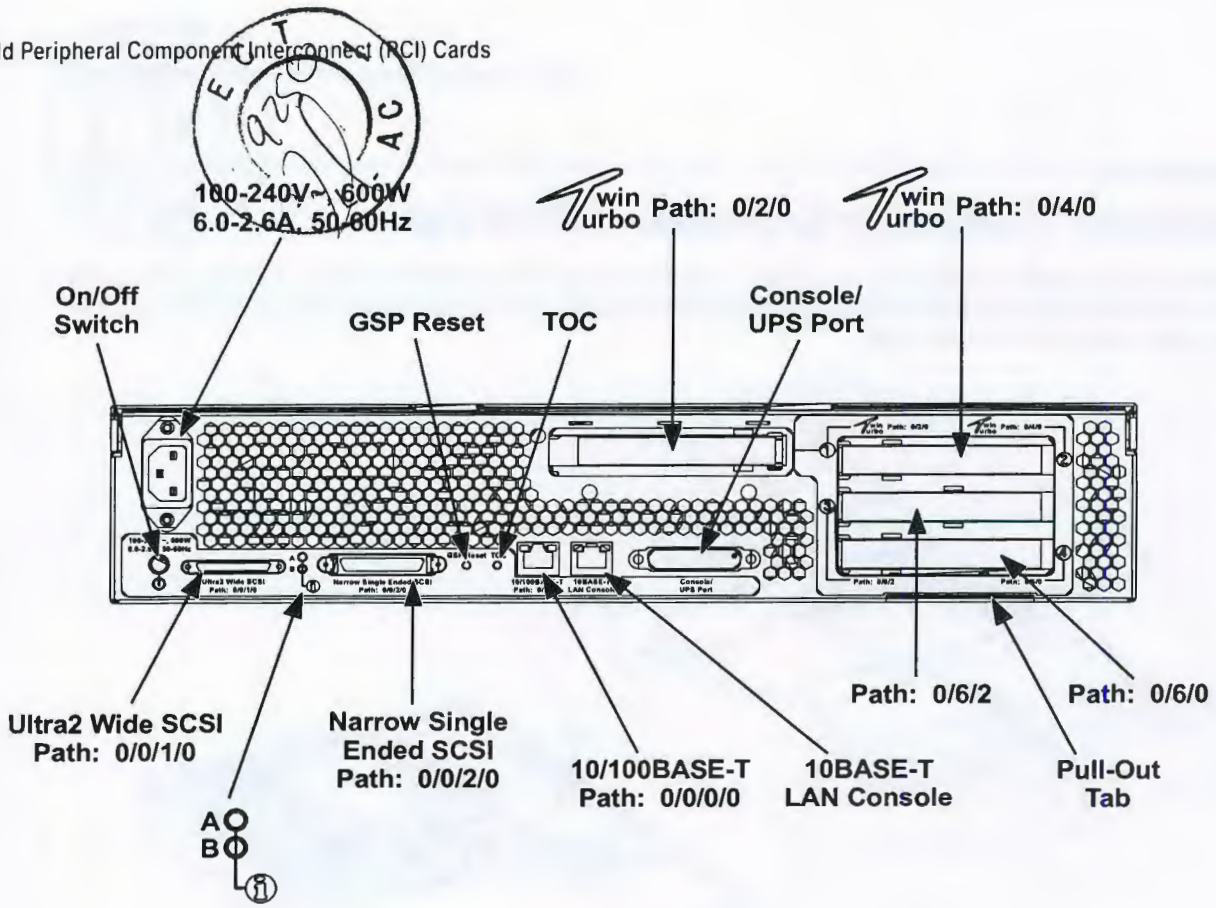
ccrr005

No.	Name	No.	Name
1	I/O Card Cage	6	I/O Card anchor screws
2	Outside I/O Card anchor screw	7	I/O Cards #2 through #4
3	Short I/O Card #1 (may be Secure Web Console)	8	I/O Backplane anchor screw
4	I/O Card Cage anchor quarter-turn fasteners	9	I/O Backplane
5	I/O Backplane disconnect lever		

- Slots 1 and 2 are Twin Turbo slots. Each Twin Turbo slot has a dedicated PCI bus and supports 32 and 64-bit PCI cards.
- Slots 3 and 4 are Turbo slots. They share a single PCI bus and support 32 and 64-bit PCI cards.

A400 servers have access to slots 1 and 2 only. A500 servers have access to all four slots. The following graphic shows the PCI slots on the rear of the server, right side.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 127
Doc.



ccrr008

New I/O Cards For rp24xx

The following table lists new I/O cards for the rp24xx.

NOTE The first HP-UX release for the new cards is 11.00.

I/O Card No.	Description
A6828A	U160 Single Port SCSI
A6829A	U160 Dual Port SCSI
A6795A	2Gb, Single Port Fiber Channel LAN
A6825A	1000BaseT Next Generation LAN
A6847A	1000BaseSX Next Generation LAN
A6386A	Hyperfabric2 (HF2) Clustering

These cards can be used in addition to the legacy cards shown below.

The following HP-UX restrictions apply regarding the installation of PCI I/O cards that contain a PCI-to-PCI bridge:

- HP-UX boot is currently not supported for cards that contain a PCI-to-PCI bridge.
- HP-UX patches are required when more than one card containing a PCI-to-PCI bridge is installed in shared slots (slots #3 and #4).

PCI cards are installed in the factory as shown in the Load Order column below, beginning with slot 1. Use the following table as a guideline for installing PCI I/O cards in the field. A system shipped from the factory may have a different configuration than one built in the field.

NOTE: All cards are not supported by A4 operating systems.

Load Order	Product Number	PCI Card Description	Part #	Max.	Boot	Future Rel.	Notes
1	A4926A	Single Port 1000BaseSX Gigabit Ethernet LAN (H)	A4926-60001	4	No	x	
2	A5483A	ATM 622 (MMF connector (H)	A5483-60001	4	No	x	
3	A6092A	Hyperfabric (H)	A6092-60001	4	No	x	
4	A4929A	Single Port 1000baseT Ethernet LAN Adapter (Gigabit ethernet copper) (H)	A4929-60001	4	No		
5	A5838A	Dual port 100baseT/X/dual port Ultra 2 SCSI Combo Interface card (F)	A5838-60001	1	No		1
6	A5506B	Quad Port 10/100B-TX LAN (F)	A5506-60101	1	No	x	1
7	A5856A	RAID Card (F)	A5856-60001	1	No		1
8	A5513A	ATM 155 (MMF connector) (H)	A5513-60001	4	No	x	
9	A5515A	ATM 155 (UTPS connector) (H)	A5515-60001	4	No	x	
10	A4800A	Single port Fast/Wide/Diff. SCSI-2 (H)	A4800-62002	4	Yes		4
11	J3525A	Dual Port serial (X25/FR/SDLC) (H)	J3525-60001	4	No		
12	A5158A	Single port Fibre Channel 1062Mb/s (H)	A5158-60001	4	Yes		
13	A5783A	Token Ring (4/16/100 Mb/s) (H)	A5783-60001	4	No	x	
14	A5230A	10/100B-TX LAN (RJ45) (H)	B5509-66001	4	No		
15	J3592A	8 Port Terminal MUX (H)	J3592-60101	4	No	x	
16	A3738A	Single Port 10/100B-TX (AUI, BNC, RJ45) (H)	A3738-60001	4	No	x	
17	J3593A	64 Port Terminal MUX (H)	J3593-60001	2	No	x	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Load Order	Product Number	PCI Card Description	Part #	Max.	Boot	Future Rel.	Notes
18	A3739B	FDDI Dual Attach Station LAN Adapter (H)	A3739-60002	4	No		
19	A5150A	Dual Port Ultra2 SCSI (F)	A5150-60001	3	Yes	x	4
20	A5149A	Single port Ultra-2 SCSI Interface card (F)	A5149-60001	3	Yes		4
21	A5486A	Public Key Cryptography (PKC) PCI (F)	A5486-60001	3	No	x	
22	A5159A	Dual Port FWD SCSI-2 (F)	A5159-60001	3	Yes	x	4
23	J3526A	Quad Port Serial (X25/FR) (F)	5063-1322	3	No	x	
24	A5858A	Secure Web Console PCI Card (H) (Optional)	A5858-70001	1	No		2
25	A6150	PCI 2D Graphics and 2 part USB adapters (H)	A6150-60001/ A6150-60002	1	No		3
(F) = Full length I/O card -- (H) = Half length I/O card. NA = Not Applicable							

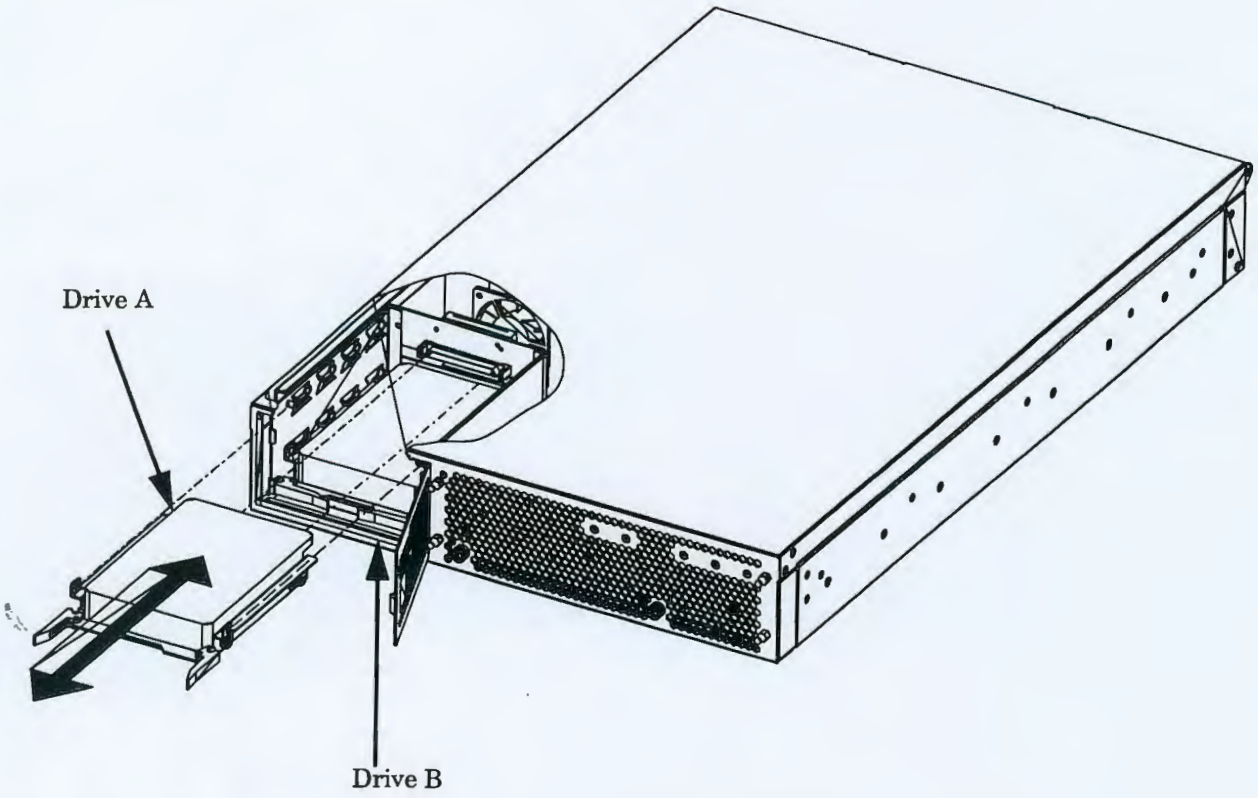
Notes:

1. Use in slot No. 2 ONLY. Cannot be used in slots 1, 3, or 4.
2. Provides web-based console capability on any PC with a browser. If needed, this card must be ordered with the A500 server. Cannot be ordered standalone. This card is not required if a system console terminal is used. Cannot have both A5858A and System Console (C1099A) on the same order.
3. Use A6150-6002 Graphics card in slot 1 only.
4. e3000 systems only.

Add Disks

rp24xx servers support two internal hard disk drives, drive A and drive B.

The following graphic depicts disk drive locations.



ccrr003

(MPE/iX does not support hotswap). It is not necessary to shutdown the HP-UX operating system or power off the server to install a new disk, but you may shutdown HP-UX and power off the server if you choose. The MPE/iX operating system needs to be shutdown prior to installing a new disk and then rebooted.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc.

Adding CPUs and Socket Cleaning

Replacement or installation of a CPU requires that the CPU chip socket be clean and uncontaminated with dirt and dust particles. The CPU chip socket must be cleaned or replaced if you:

- Replace a system board (using the CPUs from the old system board to populate the new system board).
- Add a CPU to the server.
- Remove a CPU for troubleshooting (to be replaced in the same system board).
- Remove a failed CPU and replace it with a new CPU assembly.

Tools Required

To add or replace a CPU, or to clean a system board socket and the surrounding area, you will need the following items:

- CPU socket dust cover (HP p/n A3639-40024)
- Electronic Vacuum Cleaner- ESD safe, EMI/RFI line filter, acceptable models and options are:
  1. 110V Vacuum (HP p/n 1150-5070, comes with US power cord)
  2. 220/240V Vacuum (HP p/n 1150-5071, no power cord, must order item 3 or 4)
  3. European power cord (2 meter (6foot)) (HP p/n 5184-0874)
  4. U.K. power cord (2 meter (6foot)) (HP p/n 5184-0875)
  5. Vacuum filter (0.03 micron) (HP p/n 3150-0785)

A magnifying glass, (at least 3X power) to aid in the inspection of the removed CPU socket.

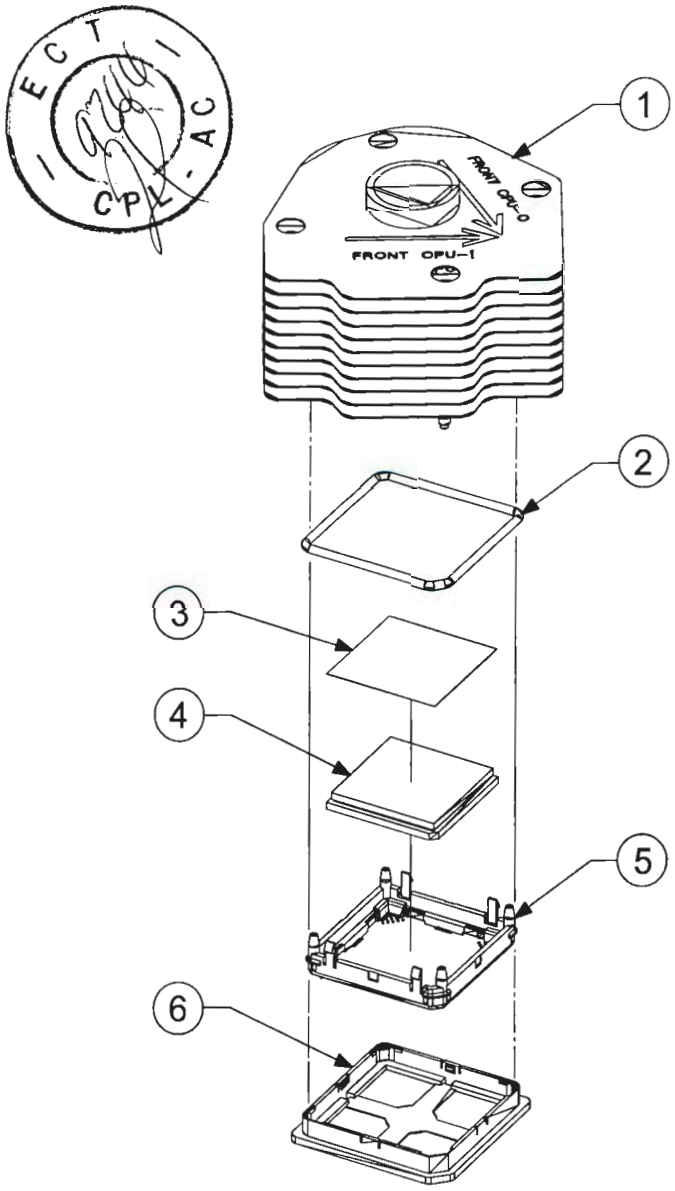
Cleaning Kit Components

The A3639-70001 CPU socket cleaning kit contains the following items.

- EMI O-ring (HP p/n 5183-3542)
- IPA pre-moistened, lint free wipes (HP p/n 5012-1138)
- thermostrate pad (HP p/n A3614-00014)
- CPU chip socket with dust cover (HP p/n 1253-0703)

The following graphic shows an exploded view of the CPU assembly, with the component names.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 596
Doc.



ccrr011

No.	Title
1	Heat Sink
2	EMI O-Ring
3	Thermostrate Pad
4	CPU Chip
5	CPU Chip Socket
6	CPU Chip Socket Dust Cover

CPU Cleaning for System Board Replacement

This section provides information for those situations where CPUs are removed and then replaced onto the same system board or onto a new system board.

1. Carefully vacuum the area surrounding the CPU to be removed and replaced.
2. Remove the CPU assembly.
3. Install the system board socket dust cover (A3639-40024) (item 6) into the empty system board socket.
4. Place the CPU assembly on its side in a clean, ESD safe area.
5. Remove the CPU assembly socket by pressing the four (two on each side) tabs holding the socket to the CPU heat sink base. The CPU chip may come off with the socket or stay attached to the heat sink. (Usually the CPU chip stays in the socket.)
6. Remove the thermostrate pad form the heat sink. It is not necessary to clean the waxy residue left behind on the heat sink and CPU chip.
7. Inspect the system board socket side of the CPU chip for any thermostrate residue. If residue is observed, clean that area with the IPA wipe.

CAUTION Do no attempt to clean the new CPU chip socket buttons.

---

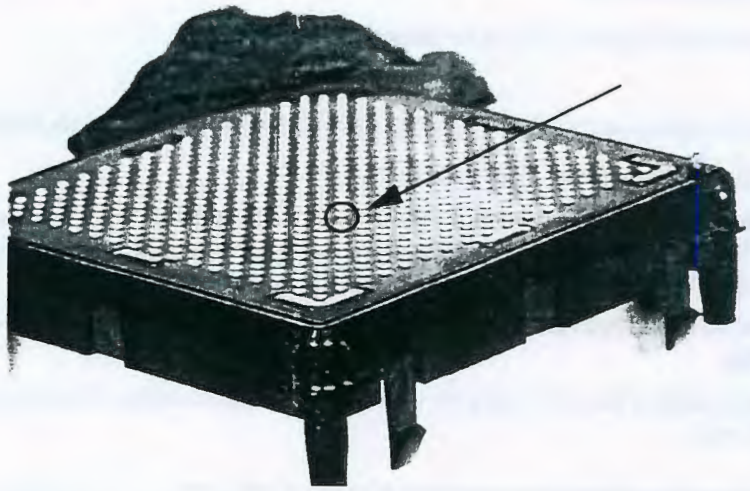
8. Place the CPU chip into the new socket. Match the cut corner of the chip with the angled corner of the socket, and be sure to have the buttons on the chip facing down. The chip should snap into the socket with light downward pressure.
9. Place the O-ring around the outside of the socket's four posts and roll it down against the corner stops.
10. Hold the heat sink assembly upside down (with the bottom up).
11. Place the new thermostrate on the copper base of the heat sink assembly, with the bevelled side down.
12. Lower the CPU chip and socket assembly onto the upside down heat sink. It only snaps in one way.

NOTE Be sure to leave the dust cover on the CPU chip until you are ready to re-install the CPU into the system board.

---

13. Remove the system board socket dust cover installed in step 3 and inspect the old socket for missing or damaged buttons. A hand-held magnifying glass is helpful. Tilt the socket at an angle. Missing buttons will show up as an irregularity in the pattern of contacts. Refer to the photograph below for an example of a socket with a missing button. If missing buttons are observed, take special care in the next step.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0687
Doc. 3698



14. Inspect the CPU socket on the system board for broken buttons or other debris. Note that it is normal for a certain amount of residue to be left behind when removing the CPU assembly. If broken buttons are observed, remove them carefully with the IPA lint free wipe. Take care to contain the debris and completely remove them from the system board socket.
15. Vacuum the system board socket site, being careful not to introduce contaminates in the process.
16. Carefully clean the system board socket with the IPA lint free wipe.
17. Install the CPU assembly into the appropriate CPU socket on the system board.

Installing the CPU

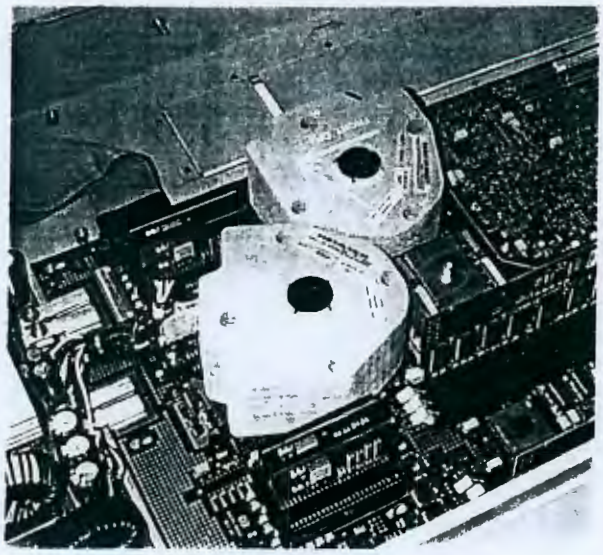
Install CPUs according to the procedure listed below:

Step 1. Carefully align the CPU notches with the socket notches and set the CPU in place.

Step 2. Tighten the four captive T-15 mounting screws that hold the CPU in place.

NOTE Tighten the four CPU mounting screws a little at a time, in a cross pattern (1, 3, 2, 4), until they are all tight.

The following picture shows both CPUs installed in a server.



NOTE The A400 system supports one CPU; the A500 supports two CPUs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 238
Doc.

System Console Configuration

The following describes the steps required to configure the HP C1099A or 700/96 terminal for VT-100 mode for operation with an rp24xx server.

C1099A VT-100 Mode Configuration.

The following procedure outlines the steps to configure the C1099A terminal for VT-100 operation.

To access the Setup menu in HPTerm emulation:

1. Press the **F10** key to display the terminal local function labels, then Press **F8** (*config keys*).

   You are now in the *Quick* (**F1**) menu.
2. Select the VT100 emulation by using the space bar to navigate through the available options.
3. Press the **ESC** key to save selected setup parameters and to exit the *Setup* menu.
4. Press the **Y** key when the blinking prompt

   `Save all? (Y/N)`

   appears in the upper right corner of the menu to save the settings in non-volatile memory.

NOTE If you enter **N** when the

`Save all? (Y/N)`

prompt appears, the changes will take effect, but will be lost if the terminal is reset or powered off.

HP700 VT-100 Mode Configuration

The following procedure outlines the steps to configure the HP700 series terminal for VT-100 operation.

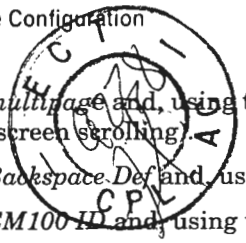
NOTE You may use either the arrow keys or the tab key to move between the setting options on the screen.

Be sure to save any configuration changes you make before proceeding to a new menu.

---

1. Press **[User System]** key.
2. Press **[config keys]** function key. **[f8]**
3. Press **[terminal config]** function key. **[f5]**
4. Move to *Terminal ID* and enter "vt100".
5. Move to *TermMode* and, using the **[Prev]** and **[Next]** keys, select "EM100".
6. Save the configuration. **[f1]**
7. Press the **[config keys]** function key. **[f8]**
8. Press the **[ansi config]** function key. **[f6]**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 139
Doc.



9. Move to *multipage* and, using the **[Prev]** and **[Next]** keys, select "yes". (Enables screen scrolling).
10. Move to *Backspace Def* and, using the **[Prev]** and **[Next]** keys, select "Backspace/Del".
11. Move to *EM100 ID* and, using the **[Prev]** and **[Next]** keys, select "EM100".
12. Save the configuration.**[f1]**

LAN Console

This section describes how to configure a notebook PC as a console via a LAN cable connection. This process uses a terminal emulator software package set to emulate a VT100 terminal.

NOTE The rp24xx server must first be configured via an HP700 system console before accessing it from a PC or UNIX system.

1. Connect a cable between the notebook PC network adapter and the 10BaseT LAN Console port on the rear of the rp24xx server.
2. Launch the terminal emulator software and set emulation to VT100.
3. Connect to the rp24xx server Guardian Service Processor (GSP) by entering its IP address and press **<ENTER>** or **<RETURN>**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
FLS. Nº 540
3698
Doc.

Secure Web Console I/O Card Replacement

The Secure Web Console (SWC) is installed in the rp24xx system as a PCI Card. This option must be included in the initial order of the rp24xx server where it will be installed at the factory during the assembly process. While not available for installation after receipt of the server, it is customer-replaceable if the factory-installed card fails during operation.

Secure Web Console Features

- **Low-level Commands** - A remote operator can exercise powerful, low-level, HP-UX and MPE/ix commands and functions.
- **Remote Server Management** - Provides secure access to the RS-232 low-level console serial port, on supported servers, via the Internet/Intranet.
- **One Person, One Console, Several Servers** - Using a browser, an operator, from a single location, can manage multiple servers, *regardless of where they are located*.
- **Simultaneous Multiple Operator Access** - Up to four operators, *in different locations,* can share the same remote server console at the same time.
- **Security** - Built-in security includes password encryption, scrambled transmission of data, and secure Java download protection.
- **Mirrored Access** - Up to four operators can simultaneously share the remote console screen and keyboard.
- **Universal Browser-based** - Supports both Netscape© v.3.0+ and Microsoft© Internet Explorer v.3.0+ Web browsers.
- **Efficient Server Access** - Operator can *bookmark* servers for multiple server lookup.
- **Upgradable** - HP Secure Web Console firmware is upgradable over the network, making it easy to add new versions and functionality.
- **Internet Standards Compliant** - Supports HTTP, FTP, TFTP, and other key Internet standards.

Secure Web Console PCI Card Replacement

The PCI card version of the SWC is a standard half-card PCI form factor. It is connected to the server by an internal bus connection in lieu of an external RS-232 connection and to the LAN by a twisted-pair cable and an RJ-45 modular plug connection. Refer to the *PCI Card Replacement* instructions for replacement procedures.

Replacing a SWC card is straightforward. However, proper configuration of the SWC card IP address, plus the complexity of the network, can present problems unless you are properly prepared before hand. It is therefore highly recommended that you:

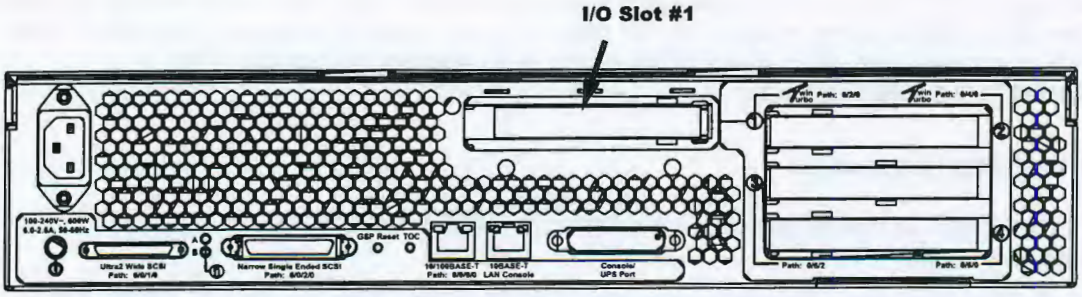
- *Read and ensure you understand the entire installation and configuration procedure* (Hardware and software) before starting.
- *Acquire all required network information* from the system administrator before starting the installation. (IP addresses, user and administrator names, passwords, etc.).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 541
3698
Doc.

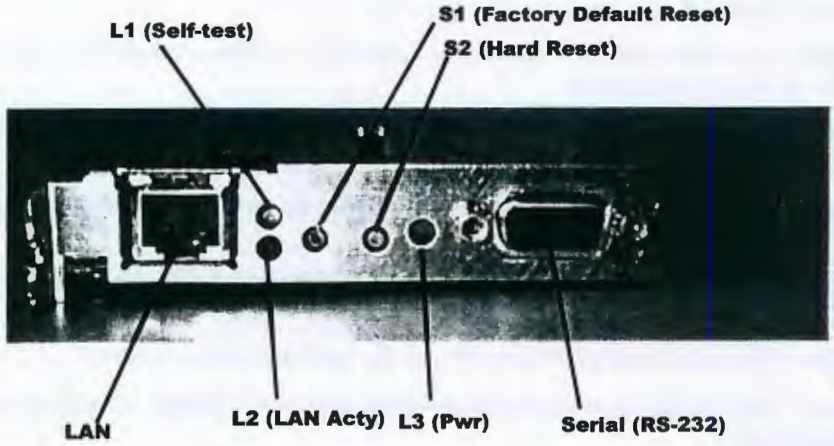
COPY

Secure Web Console PCI Card Introduction.

Since the SWC card is half-card size, it will normally be installed on the server rear bulkhead in I/O slot #1 as shown below:



A picture of the SWC card I/O interface connector is included to show location and identity of LEDs, buttons, and ports:



Title	Description
LAN Port	Plug-in for Local Area Network (LAN) connector.
L1 (Self-test)	Lights when self-test is performed.
L2 LAN Activity	When lit, indicates activity between LAN and the SWC card.
L3 Power	When lit, indicates power to the SWC card.
S1 Factory Default Reset	Only effective when pressed simultaneously with S2.
S2 Hard Reset	Momentarily cuts power to the SWC.
Serial Port (RS-232)	Plug-in for RS-232 connector.

NOTE If you press and hold the S2 (Hard Reset) switch, press the S1 (Factory Default Reset) switch, then release S2 while continuing to hold S1, the SWC card will reset to factory specifications.

Pre-Installation Considerations

The following paragraphs provide an outline of the pre-installation items you should address before starting SWC card replacement.

- Obtain an IP address to be assigned to the SWC card.
- Obtain the subnet mask to be assigned to the SWC card.
- Obtain the gateway address for the SWC card. If a gateway address is unavailable use the SWC card's IP address.
- Know the name of the system to be administered by the SWC card.
- Have internet access available to access the on-line installation and configuration procedures, and the troubleshooting tools.
- Ensure that your browser is on the Supported Browsers list
- Configure your Web Browser software options as follows:

  — ***For Microsoft Internet Explorer©:***
  • Turn off the JIT Compiler — (Deselect the **[Java JIT Compiler Enabled]** preferences box).

  — • Disable Proxies (Until final IP address is assigned) or add the 192.0.0.192 to the proxies list.

  — ***For Netscape Communicator©:***
  • Disable Proxies (Until final IP address is assigned) or add the 192.0.0.192 to the proxies list.

NOTE How these configuration settings are made varies with browsers and versions. For specific instructions on how to set these options, check the documentation specific to your browser.

Installing Multiple Secure Web Consoles.

All network devices require unique IP addresses to operate correctly. All SWC cards ship from the factory with the same default IP address: 192.0.0.192.

If another device on the network is using the same address (e.g. 192.0.0.192) the results of the installation will be *unpredictable.*

Dynamic Host Configuration Protocol (DHCP) and the Secure Web Console.

Every computer on the internet or intranet has a unique TCP/IP number/address. Traditionally, TCP/IP numbers are assigned by hand. DHCP is a protocol that allows the assignment of IP addresses *on-the-fly,* for a single session use, from a pool of numbers that the DHCP server controls. Typically, you can use DHCP to preconfigure SWCS permanent network parameters. For more information, go to the SWC DHCP web page at: http://www.docs.hp.com/hpux/onlinedocs/hw/swc/install/00096I/index.htm

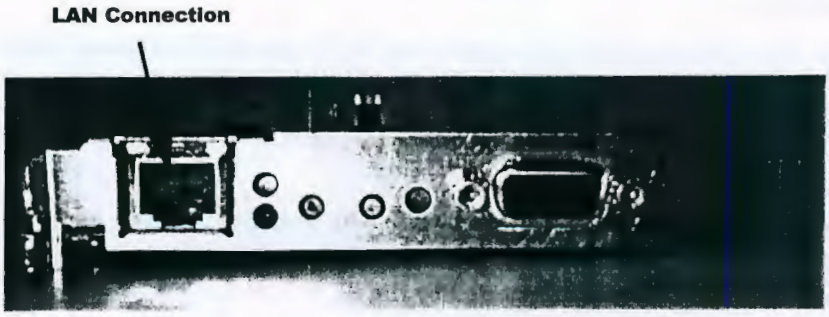
NOTE Only DHCP on HP-UX is supported.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 145
Doc.

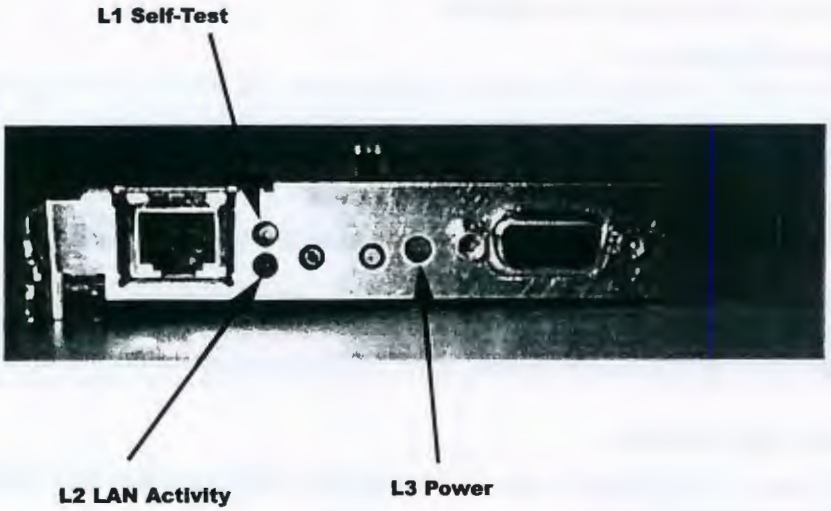
Initial Cable Connections

To make the cable connections, proceed as follows:

Step 1. Connect the SWC card to the Intranet/internet (LAN).



Step 2. Observe the LEDs on the SWC card rear bulkhead connector.



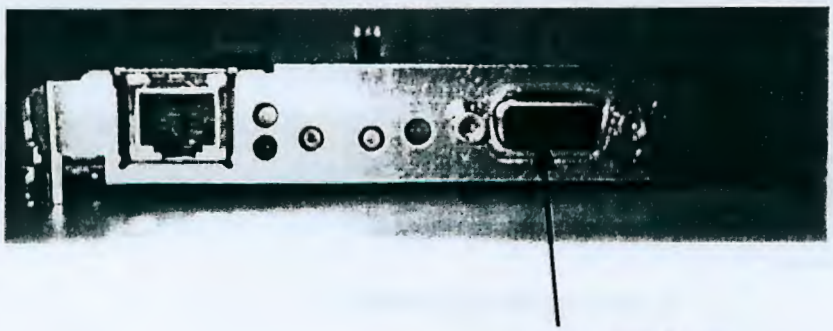
LED Indications

Solid Amber	Self-Test in progress
Amber Off	Self-Test completed
Amber Stays On	Self-Test Failed
Flashing Green (LAN)	Network Activity
Solid Green (Power)	Power on

CAUTION For system security, initial configuration must be completed *before* making the serial connection between the SWC card and the server's console port.

Failure to follow this precaution can result in root level access being available to any level of SWC user.

Step 3. Connect the server's console to the SWC card via the RS 232 Serial port.



RS 232 Serial Port

Step 4. Perform Initial Configuration of the SWC card.

a. Ensure that no other devices (printers, etc.) are connected *on the same local subnet* by disconnecting the LAN cable from the SWC and using the *Ping* command as follows:

```
C:\ ping 192.0.0.192
```

It will time out.

b. At a command line prompt, enter the following:

```
C:\route add 192.0.0.192 xx.xx.xx.xx.xx
```

Where *xx.xx.xx.xx.xx* is the IP address of your PC or Unix workstation.

c. Reconnect the LAN cable to the SWC card and use a PC or Unix Workstation and a web browser. Verify that you can access the SWC at its default IP address using the *Ping* command as follows:

```
C:\ping 192.0.0.192
```

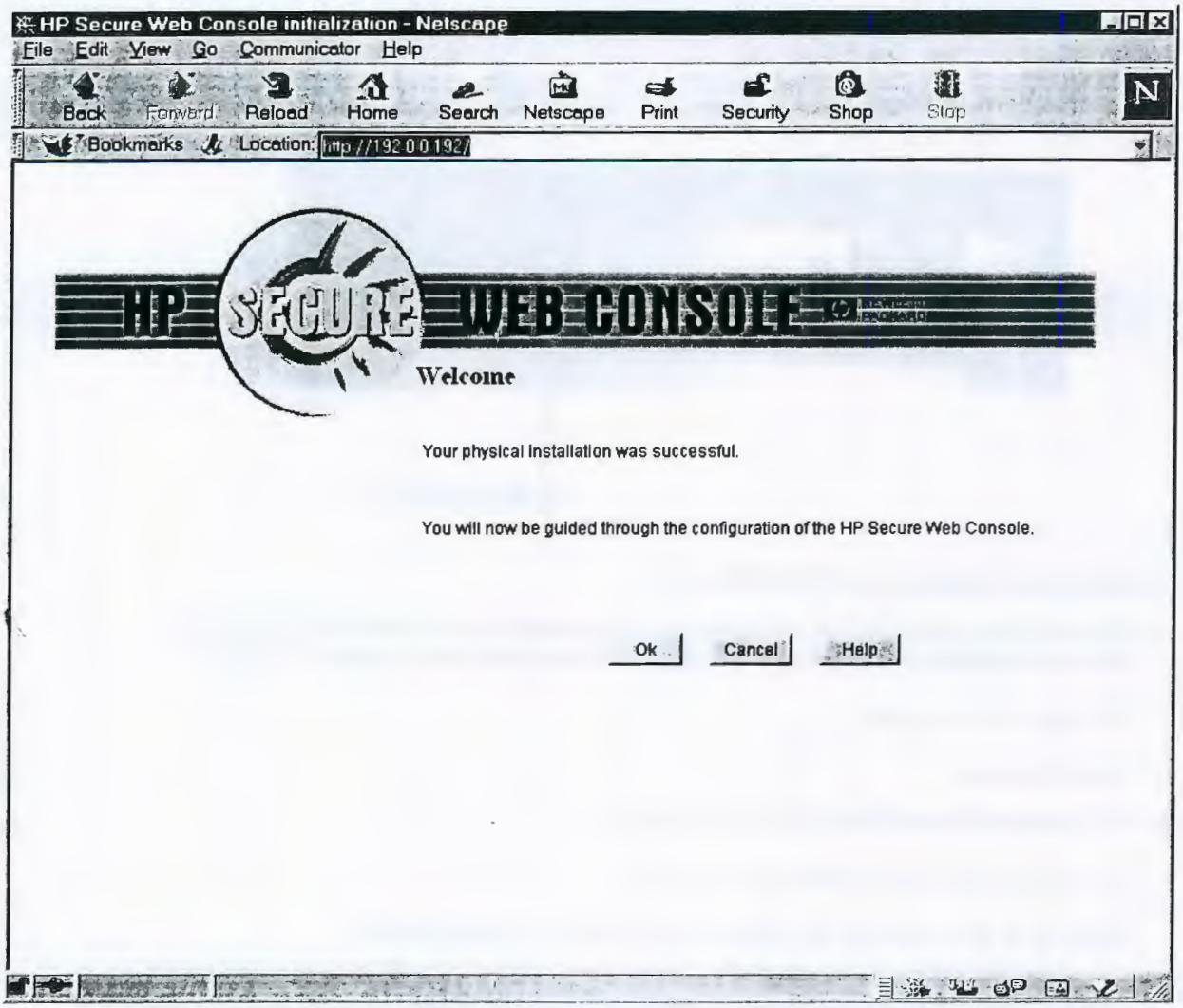
It will indicate connection with the SWC card at IP 192.0.0.192

Step 5. Create the first SWC administrator account.

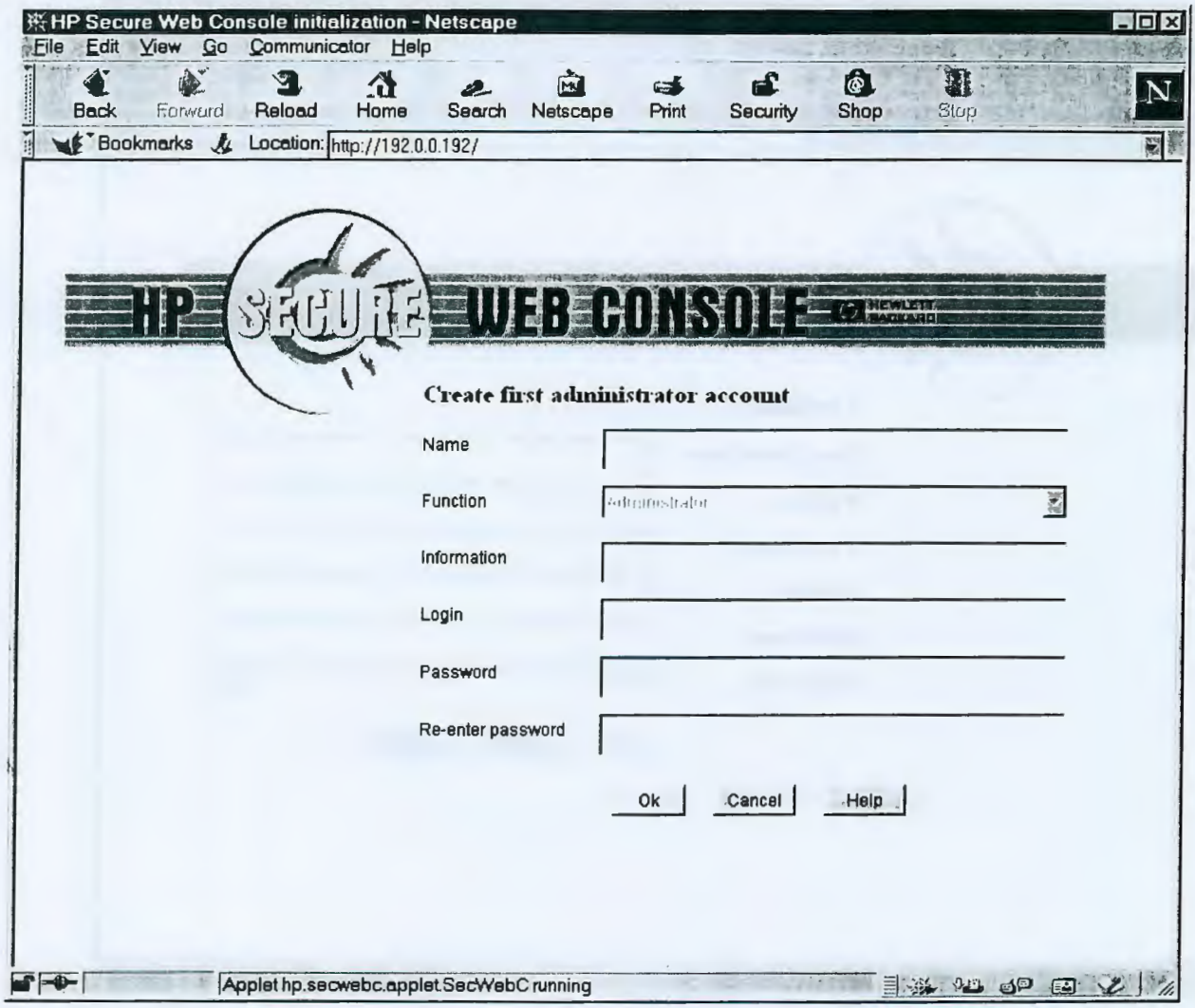
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 147
Doc. 3698

NOTE The SWC requires creation of the first administrator account before proceeding further.

a. Using a web browser, access the SWC at the default IP address (192.0.0.192).



b. To create the first SWC administrator account, fill in the prompts shown in the following illustration:



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 541
Doc. 3

NOTE The adapter cable (p/n A5858-63001) connects between the SWC and the console cable (p/n A5191-63001).

Step 8. SWC card configuration is complete.

Step 9. Use [Zoom In] or [Zoom Out] to adjust the size of the display window.

Step 10. Refer to [Help] or [Tour] to review SWC card features and functions.

Secure Web Console System Information

For technical documentation about the Secure Web Console, refer to the following URL:

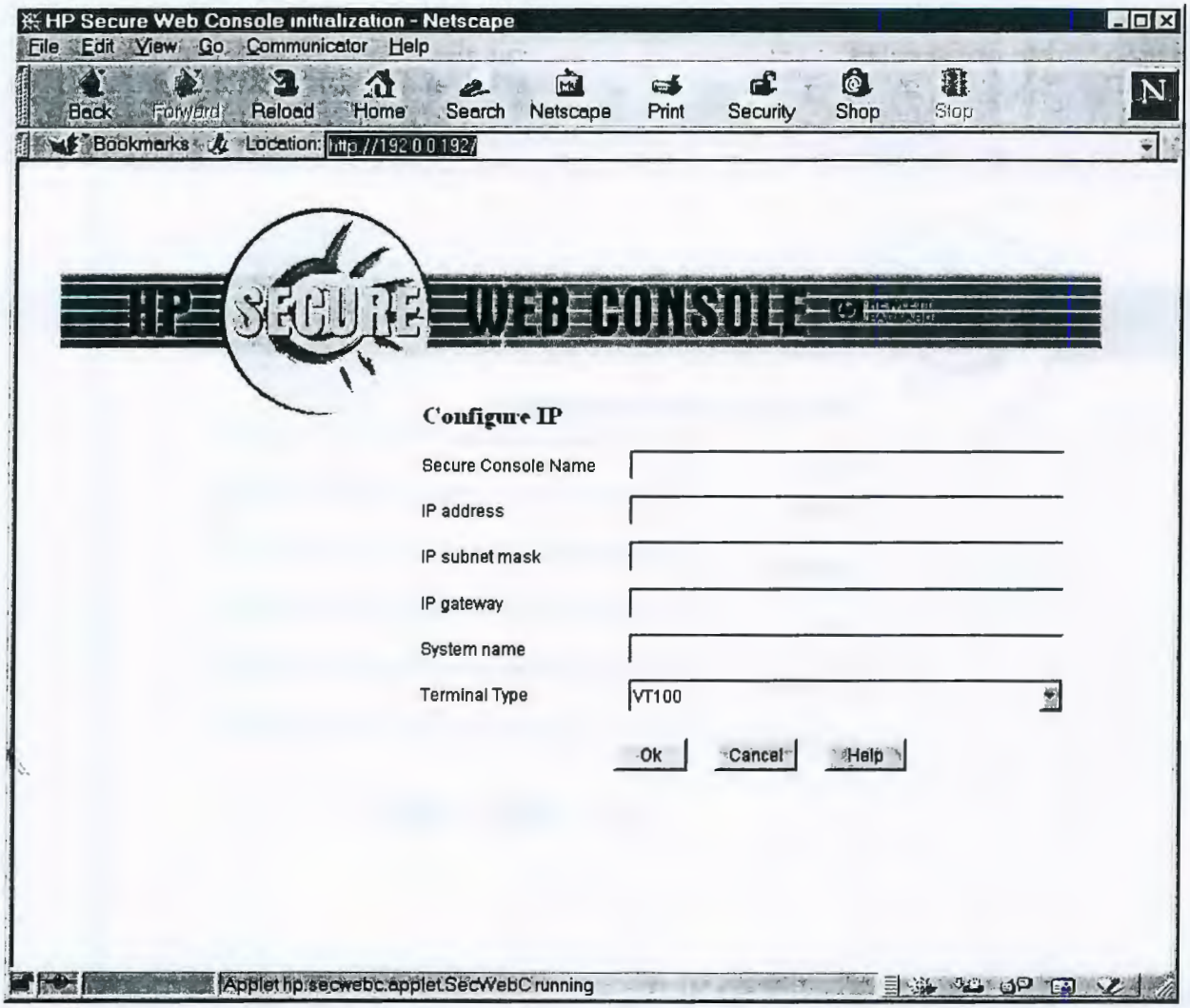
http://www.docs.hp.com

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 151
Doc.

8 Troubleshooting the Server

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 546
Doc.

c. To configure the network parameters for the SWC, fill in the prompts shown in the following illustration:



d. When all necessary data is entered, click on [OK] to reboot the SWC.

Step 6. Using a web browser, connect to the SWC card, using:

- the newly assigned IP address, and
- the newly created administrator log-in and password.

NOTE It may take as much as 45 seconds to gain initial access to the SWC card.

Step 7. Connect the serial cable between the SWC card and the server's console port.

Chassis Code to Customer Replaceable Unit (CRU) Decode

This is a guide to identify failing CRU's from the Error Chassis Logs. The guide includes the following information:

- "Accessing Error Chassis Logs"
- "Key Identification Fields for Error Chassis Logs"
- "Cross-Referencing Chassis Log Errors to A400/500 CRU's."

Accessing Error Chassis Logs

Execute the following steps to access the Error Chassis Logs.

1. At the system console prompt, type **CTRL B** (this will bring up the gsp login screen)
2. Type in the Service Processor Login and Password (this will give you a GSP prompt)
3. At the prompt,

   `GSP>`, type **SL** (this will take you to the support logs)
4. At the prompt,

   `Which buffer are you interested in:`
   `Incoming, Error, Current boot, Last boot? (I/A/E/C/L)`, type **E** (for error logs)
5. At the prompt,

   Do you want to set up filter options on this buffer? (Y/[N]), type **N**
6. At this point, the most recent Error Log Entry (Log Entry #0) will be displayed. A carriage return after this will display the next log entry. Type **Q** to stop displaying the log entries.
7. At the prompt,

   `GSP>`, type **CO** to return to the console

Key CRU Identification Fields for Error Chassis Logs

The following fields (bold in the sample error log entry) are useful for FRU identification.

Alert Level:	How the problem has affected the system operation.
Source:	What major part of the system the alert is referring to (i.e., platform, memory, processor, etc.).
Source Detail:	What sub-part of the system the alert is referring to (i.e., cabinet fan, DIMM, high voltage DC power, etc.).
Source ID:	Specific CRU referred to in Source and Source Detail (i.e., fan #1).
Problem Detail:	Specific problem information (i.e, power off, functional failure, etc.).
Timestamp:	When the problem occurred.

Cross-Referencing Chassis Log Errors to A400/A500 CRU's

Use the following table to identify the failing CRU from the Chassis Log information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 54
Doc. 3698

1. Read the Chassis Log entry.
2. Match the **SOURCE**, **SOURCE DETAIL**, **SOURCE ID**, and **PROBLEM DETAIL** values found in the Chassis Log entry with the appropriate values in the table.
3. Read the table from left to right.

Table 7-1

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**CRU**	**Action to Take**
1 - Processor	Not Applicable (N/A)	N/A	N/A	Processor	Not a CRU, Contact HP support.
2 - Processor Cache	Not Applicable (N/A)	N/A	N/A	Processor	Not a CRU, Contact HP support.
3 - PDH	Not Applicable (N/A)	N/A	N/A	System Board	Not a CRU, Contact HP support.
4 - Power	1 - AC Mains	N/A	9 - Power Off	AC Power	Check that the AC is being supplied to power supply.
4 - Power	3 - Low Voltage DC Power Converter	N/A	N/A	CPU Support Module	Replace the Processor Support Module (DC - DC Conveter)
4 - Power	4 - High Voltage DC Power	Power Supply #	N/A	Power Supply	Not a CRU, Contact HP support.
6 - Platform	3 - Cabinet Fan	N/A	N/A	Fan	Replace the Fan assembly.
6 - Platform	6 - Service Processor	N/A	N/A	GSP PCA	The Service Processor is on the GSP I/O board. Replace the GSP
6 - Platform	7 - Power Monitor	N/A	N/A	System Board	Not a CRU, Contact HP support.
7 - Memory	1 - Controller	N/A	N/A	System Board	Not a CRU, Contact HP support.
7 - Memory	4 - SIMM or DIMM	N/A	N/A	Memory DIMM	Isolate to failing DIMM using BCH (IN, ME) and ODE memory diagnostic.

Table 7-1 (Continued)

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**CRU**	**Action to Take**
8 - I/O	6 - Disk	N/A	Various Values	Disk Subsystem	Use BCH commands and ODE diagnostics to check disk subsystem.

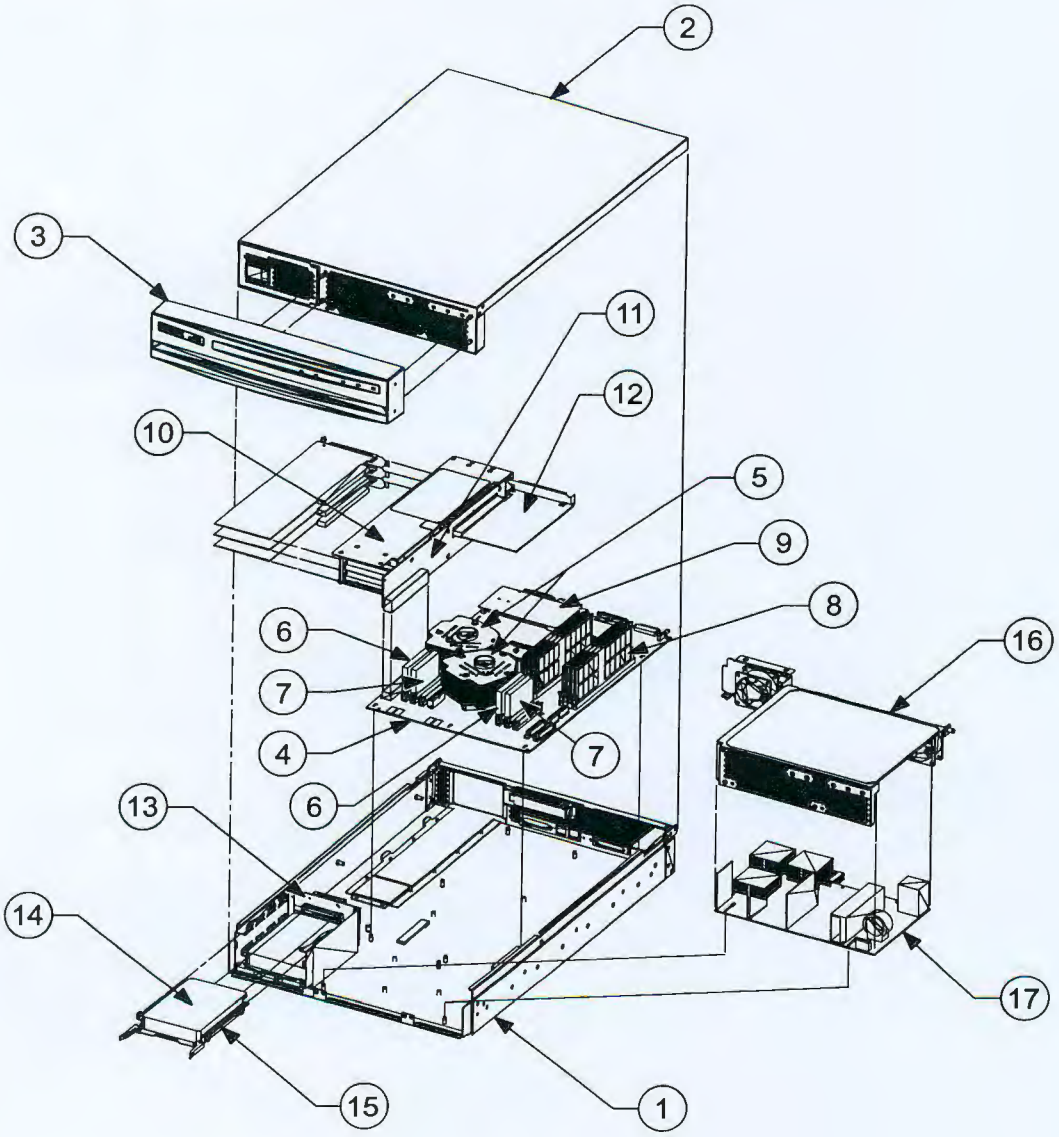
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3
Doc. 3698

9 Server Component Removal and Replacement Procedures

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 549
Doc. 3698

Customer Replaceable Unit (CRU) Physical Location

This section contains views of the rp24xx server. The locator numbers in the diagrams correspond to the numbers in the CRU Part Number section.



ccrr009

NOTE Components numbered 1, 4, 5, 13, 16. and 17 are not customer replaceable and do not appear in the Customer Replaceable Unit (CRU) Part Numbers section. They are included in this illustration for continuity, only.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Customer Replaceable Unit (CRU) Part Numbers

The following tables list all Customer Replaceable Units (CRUs) for the rp24xx server. CRUs may be removed or replaced by either the customer or by qualified HP field engineering personnel. Table 1 lists both new and exchange part numbers. Table 2 lists only the new part numbers for non-exchange CRUs.

Exchange CRUs

Product #	New Part #	Exch. Part #	Description	Loc. #
A6114A	A6114-60001	A6114-69006	2048 MB Memory DIMM	8
A5841A	A5841-60001	A5841-69001	1024 MB Memory DIMM	
A5840A	A5840-60001	A5840-69001	512 MB Memory DIMM	
A5572A	A5572-60002	A5572-69002	128 MB Memory DIMM	
A5505A	A5505-60001	A5505-69001	9 GB Disk Drive	14
A5531A	A5531-60001	A5531-69001	18 GB Disk Drive	
A6089A	A6089-67001	A6145-69001	36 GB Disk Drive	
A5570A	A5570-60002	A5570-69002	Guardian Service Processor	9

Non Exchange CRUs

Part #	Description	Loc #
A5570-60003	PCI I/O Backplane	11
A5570-60005	Secure Web Console PCA	12
A5570-00002	Disk Carrier	15
0950-3821	DC-DC Converter - Master	6
0950-3822	DC-DC Converter - Slave	7
A5570-62003	I/O Card Cage Chassis	10
A5570-62006	Plastic Front Bezel	3
A5570-67007	Chassis Top Cover	2
A5570-84001	rp2450 Name Plate	N/A
A5191-63001	Console-Remote-GSP Cable	N/A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 551
Doc. 3698

Front Bezel Removal

The rp24xx server does not have to be turned off to remove the bezel.

WARNING **Do not attempt to lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency. Failure to heed this warning may result in personal injury and/or permanent damage to the server.**

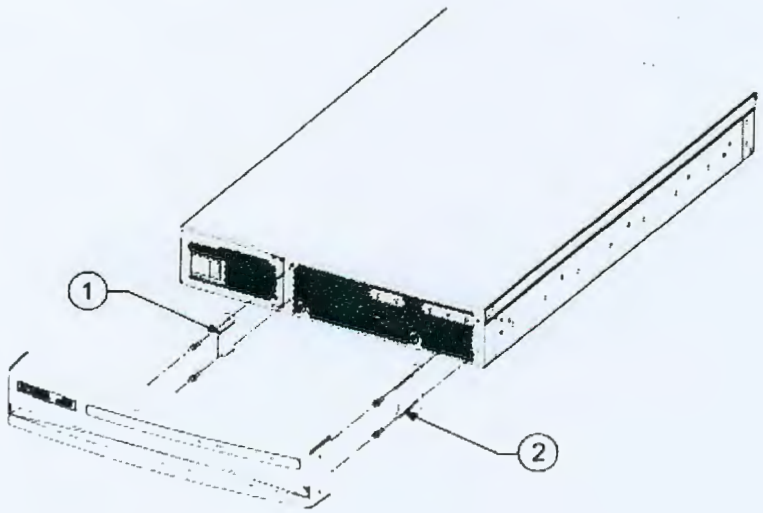
Removing the bezel provides access to the following:

- HotPlug Disk Drive access door.
- Two knurled thumbscrews that secure the server cover.

To remove the bezel, grasp the bezel at the sides and pull straight out until it is free of the bezel retainers and ball-posts on the server.

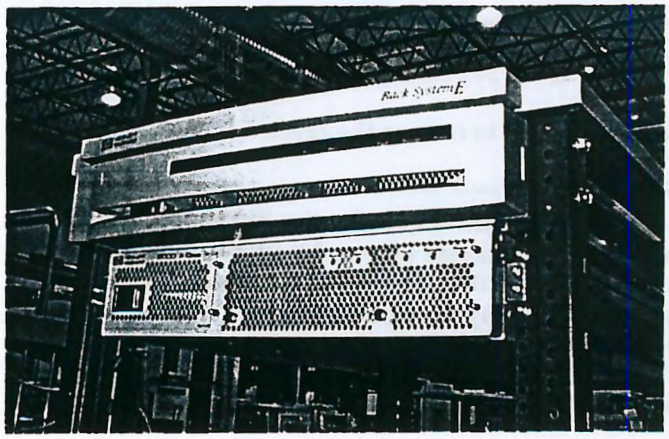
CAUTION Pull the bezel straight out. Do not twist or wiggle from side-to-side any more than necessary to keep from damaging the bezel sockets.

The following illustration shows a server and bezel with the bezel retainers and ball posts in an exploded view.



The following picture shows one server with the front bezel attached and one server without.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.



Front Bezel Replacement

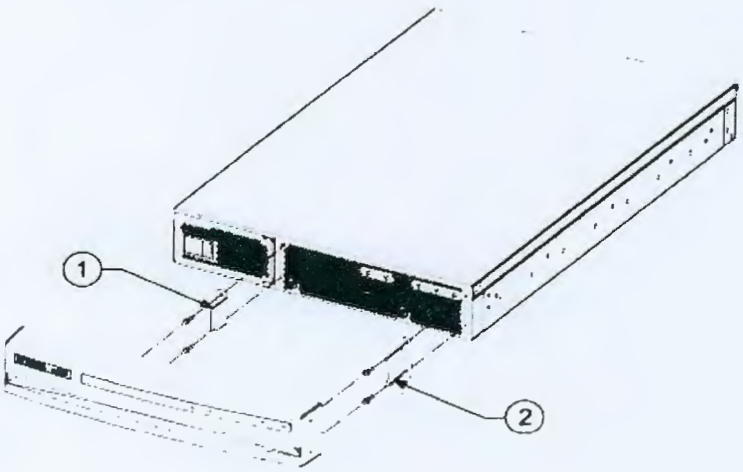
The rp24xx server does not have to be turned off to replace the bezel.

WARNING **Do not lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency.**
Failure to heed this warning may result in personal injury and/or permanent damage to the server.

To replace the bezel, grasp the bezel at the sides and align the bezel sockets with the bezel retainers and ball-posts on the server and push straight in. The bezel will lock into place.

CAUTION During replacement, do not twist or wiggle the bezel from side-to-side any more than necessary to keep from damaging the bezel socket.

The following illustration shows a server and bezel with the bezel retainers and ball posts in an exploded view.

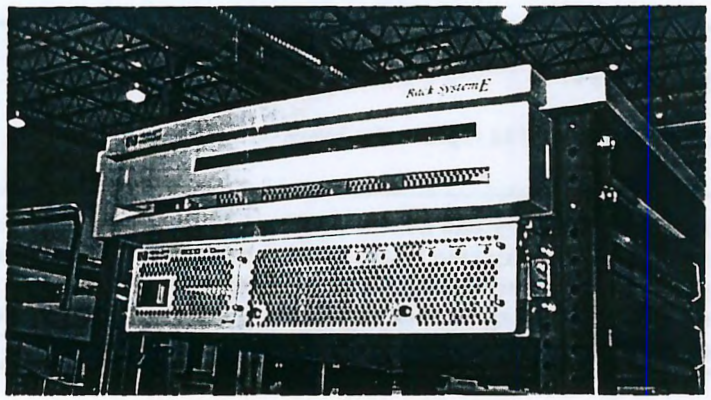


As you are facing the front of the server, item 1 is the left bezel retainer with two ball posts, and item 2 is the right bezel retainer with two ball posts.

CAUTION Left and right bezel retainers are NOT interchangeable.

The following picture shows one server with the front bezel attached and one server without.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 553
3698
Doc.



Server Cover Removal

The cover that protects rp24xx server components is secured by two thumbscrews and, when released, slides forward for removal.

To remove the cover, perform the following procedures:

Step 1. Remove the front bezel.

WARNING **There is a safety interlock between the front of the server cover and the Power Supply. When the cover is taken off, power is automatically removed from the server if power cords were not detached previously.**

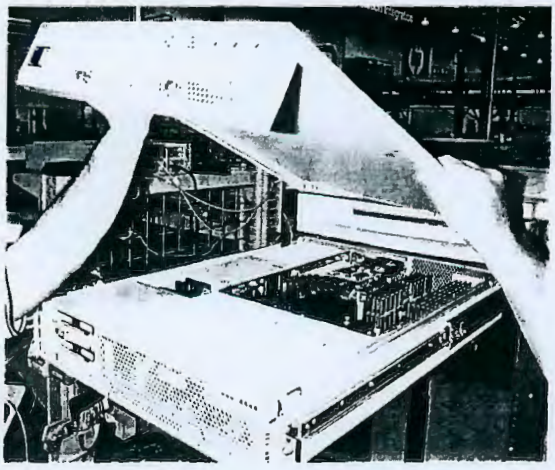
DO NOT attempt to defeat this interlock. Doing so will expose you to high levels of electrical amperage that can cause serious injury or death.

Step 2. Unfasten the two captive knurled thumbscrews located near the bottom edge of the front of the server cover.

Step 3. Grasp the thumb screws and pull the cover toward you. Slide the cover approximately 2.5 MM (1 in.) then lift the cover front to clear the notches on each side of the server. Set the cover aside.

CAUTION The server weighs approximately 23 kg (50 lbs). Take necessary precautions to prevent muscle strain when lifting and carrying the server.

The following graphic shows the server cover suspended over the server.



RQS nº 03/2005 - CN
CPMI -- CORREIOS
Fls. Nº 5
Doc.

Server Cover Replacement

The cover that protects rp24xx server components must be raised in front and positioned on top of the side chassis panels then lowered and slid into the back chassis panel. The cover is secured by two thumbscrews attached to the front chassis panel.

To replace the cover, perform the following procedures:

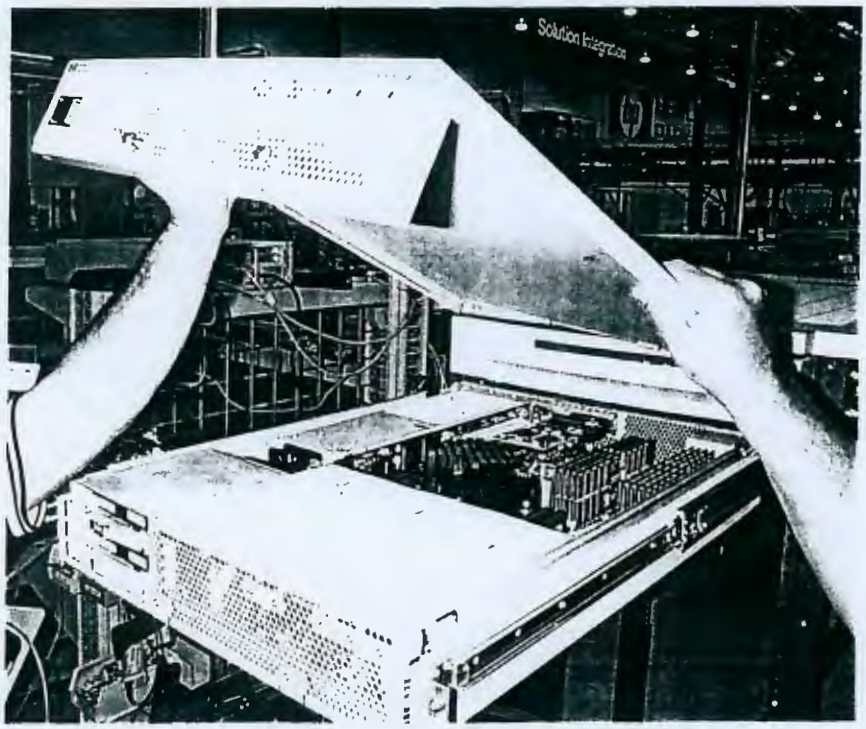
Step 1. Tilt the cover front up slightly and position it on top of the chassis side panels approximately 2.5 MM (1 in.) from the rear of the server chassis.

Step 2. Lower and slide the cover back over the notches on each side of the front of the server and seat it against the rear chassis panel.

Step 3. Fasten the two captive knurled thumbscrews located near the bottom edge of the front of the server cover.

CAUTION The server weighs approximately 23 kg (50 lbs). Take necessary precautions to prevent muscle strain when lifting and carrying the server.

The following graphic shows the server cover suspended over the server.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3693
Doc.

HotPlug Disk Drive Removal (HPUX Systems Only)

The disk drives (up to two) are located at the front left side of the server (as you are facing it). When proper software and hardware procedures are followed, these disk drives can be removed and replaced while the server is running.

NOTE MPE/iX does not support hotswap. Do not use these procedures on HP e3000 servers.

The procedures in this section are in two parts, a software HotPlug procedure to prepare the drive for removal and the hardware procedures for physically removing the device from the server.

Before starting these procedures, you must have an up-to-date configuration backup file. Configuration backup is performed by default each time an LVM command changes the LVM configuration. The default backup file path is:

```
/etc/lvmconf/base_vg_name.conf
```

The replacement disk drive must be the same product ID as the disk drive that is being replaced.

NOTE HP often uses different manufacturers for disks that have the same product number. The HotPlug manual procedure will not update the disk drivers internal information to that of the replaced disk drive.

The replacement disk drive will have the same capacity and blocksize as the defective disk because they have the same product number. The only field that can be incorrect is the string specifying the vendor's name. This will not affect the behavior of the LVM. If you desire to update the manufacturer's name, the disks volume group must be deactivated and reactivated.

HotPlug Software Procedure

NOTE The HotPlug software procedures for Disk Drive removal/replacement described below are for a mirrored boot disk configuration only. If your configuration differs from this, these procedures may not be valid. Consult your System Administrator or contact the HP Response Center for assistance.

Perform these software procedural steps to replace a HotPlug disk drive device:

Step 1. Determine whether or not the LVM found the physical volume to be defective when the volume group was activated.

If the volume was defective when the volume group was activated, *vgchange* would have generated the following message to the console:

```
WARNING

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
VOLUME "/DEV/DSK/cXtXdX"

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 550
3698
Doc.

```
VOLUME "/DEV/DSK/cXtXdX"
THE PATH OF THE PHYSICAL VOLUME REFERS TO A DEVICE THAT DOES NOT
EXIST, OR IS NOT CONFIGURED INTO THE KERNAL.
```

If you are unsure of the status of the *vgchange*, you may check if this occurred by typing the *vgdisplay* command: *vgdisplay <VG name>*. For example:

```
# vgdisplay /dev/vg00
```

If you see these messages, the disk was defective at the time the volume group was activated. Remove the bad disk as described in the *HotPlug Hardware Procedure* section, then follow the instructions in *Disk Drive Replacement* for replacing the disk and perform the Hot Swap Procedure for Unattached Physical Volumes described there. Otherwise, your disk drive became defective after the *vgchange* and you must continue with step 2 of this section.

Step 2. Display the names of all the logical volumes on this volume group using the *vgdisplay* command. For example:

```
#vgdisplay /dev/vg00
```

Step 3. Determine which logical volumes have mirrors by using the *lvdisplay* command. For example:

```
#lvdisplay /dev/vg00/lvol# | grep -ie "LV Name" -e
"Mirror"
```

Step 4. Determine the *pvkey* for the mirrored logical volume, again using the *lvdisplay* command with the *-k* option. Compare the output to the *lvdisplay* command with the *-v* option to determine the device file to *pvkey* mapping. For example,

```
# lvdisplay -v -k /dev/vg00/lvol1

--- Logical volumes ---
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
LV Permission               read/write
LV Status                 available/syncd          Mirror copies
1          Consistency Recovery       MWC              Schedule
parallel     LV Size (Mbytes)           256            Current LE
64       Allocated PE              128        Stripes                  0
Stripe Size (Kbytes)       0               Bad block               off
Allocation                strict/contiguous        IO Timeout (Seconds)
default             --- Distribution of logical volume ---PV Name           LE
on PV  PE on PV  /dev/dsk/c1t6d0    64       64       /dev/dsk/c2t6d0    64
64

--- Logical extents ---LE        PV1        PE1   Status 1 PV2          PE2
Status 2 00000     0       00000 current  1           00000 current  00001
0        00001 current  1            00001 current  00002     0        00002
current  1          00002 current  00003     0       00003 current  1
00003 current  00004     0        00004 current  1            00004 current
00005     0       00005 current  1          00005 current  00006     0
00006 current  1           00006 current  00007     0        00007 current
1            00007 current  00008     0         00008 current  1
00008 current  (etc.)
# lvdisplay -v /dev/vg00/lvol1--- Logical volumes ---LV Name
/dev/vg00/lvol1VG Name                    /dev/vg00LV Permission
```

```
read/write   LV Status                    available/syncd          Mirror
copies              1          Consistency Recovery       MWC
Schedule                   parallel    LV Size (Mbytes)          256
Current LE                    64        Allocated PE               128
Stripes                    0      Stripe Size (Kbytes)       0
Bad block                     off          Allocation
strict/contiguous          IO Timeout (Seconds)        default             ---
Distribution of logical volume ---PV Name            LE on PV  PE on PV
/dev/dsk/c1t6d0    64        64        /dev/dsk/c2t6d0    64        64
--- Logical extents ---LE    PV1              PE1   Status 1 PV2
PE2   Status 2 00000 /dev/dsk/c1t6d0    00000 current  /dev/dsk/c2t6d0
00000 current  00001 /dev/dsk/c1t6d0    00001 current  /dev/dsk/c2t6d0
00001 current  00002 /dev/dsk/c1t6d0    00002 current  /dev/dsk/c2t6d0
00002 current  00003 /dev/dsk/c1t6d0    00003 current  /dev/dsk/c2t6d0
00003 current  00004 /dev/dsk/c1t6d0    00004 current  /dev/dsk/c2t6d0
00004 current  00005 /dev/dsk/c1t6d0    00005 current  /dev/dsk/c2t6d0
00005 current  00006 /dev/dsk/c1t6d0    00006 current  /dev/dsk/c2t6d0
00006 current  00007 /dev/dsk/c1t6d0    00007 current  /dev/dsk/c2t6d0
00007 current  00008 /dev/dsk/c1t6d0    00008 current  /dev/dsk/c2t6d0
00008 current
```

The p*vkey* (0 or 1 in this example) shown in the first command maps to the device file names (/dev/dsk/c1t6d0 or /dev/dsk/c2t6d0) in the second command under columns PV1 and PV2, respectively.

Step 5. Reduce any logical volumes that have mirror copies on the faulty disk drive so that they no longer mirror onto that disk drive (note the *-A n* option):
 # lvreduce -m 0 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>& (for one-way mirroring)
OR
 # lvreduce -m 1 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>& (for two-way mirroring).

For example:
 # lvreduce -m 0 -A n -k /dev/vg00/lvol4 /dev/dsk/c2t4d0 1&

The following message will appear:

```
Logical volume /dev/vg00/lvol4 has been successfully reduced.
lvlnboot: Logical Volume has no extents
```

It is important to include the ampersand (&) at the end of the command line. This *lvreduce* process will hang, and you will need terminal control to kill the command. Once the "successfully reduced" message has been generated, manually kill the process, using the kill -9 command.

a. Use the *ps* command to find the PID for the *lvreduce* process.

```
# ps -ef | grep lvreduce
```

b. Stop the process. (This may take several minutes before the process finally ends.

```
# kill -9 <PID>
```

Step 6. Repeat steps 4 and 5 for all logical volumes.

Step 7. With all logical volumes reduced, now reduce the volume group using the *vgreduce* command. For example:

```
# vgreduce /dev/vg00 /dev/dsk/c2t6d0
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

The *vgreduce* process may take a long time to complete. Do NOT kill this process.

Step 8. Update the disk BDRA using the *lvlnboot* command.

```
# lvlnboot -R
```

HotPlug Hardware Procedure

CAUTION (MPE/iX does not support hotswap). Disk Drives can be removed or installed with the server still powered on. This is referred to as a "manual HotPlug". However, DO NOT remove a HotPlug disk drive until all prior software procedures have been completed. The MPE/iX operating system needs to be shut down prior to installing a new disk and then rebooting.

To remove a bad disk drive from the server, perform the following steps:

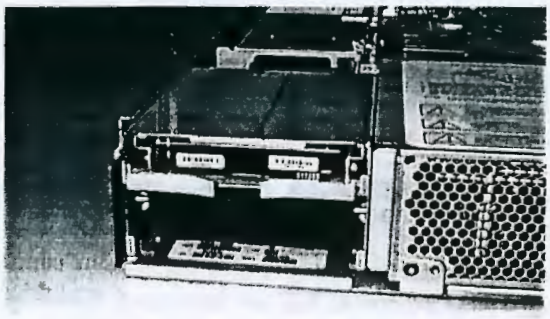
Step 1. Remove the front bezel.

Step 2. On the left side of the front of the server you will see a door with a spring-loaded latch holding it shut. Open the door to expose the disk drive slots.

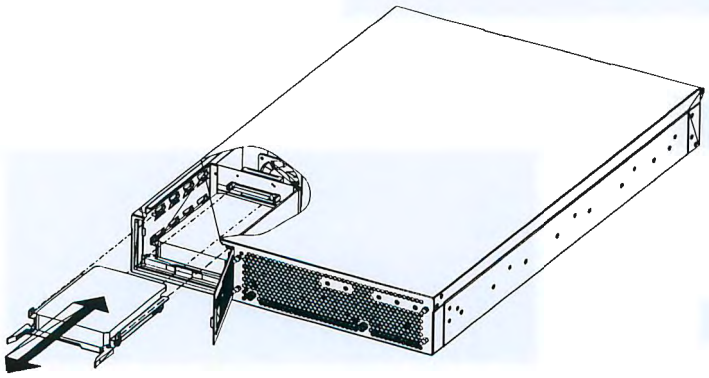
Step 3. Perform the following steps in the order shown:

1. Pull out on the extraction levers on each side of the selected disk drive to unlock it.
2. Pull gently on the levers to pull the disk drive partially out of its slot
3. Wait 10 seconds for the drive to spin down.
4. Grasp the disk drive, pull it completely out of its slot, and set it aside.

The following photograph shows a HotPlug disk installed in the disk housing.



The following graphic shows the location of the HotPlug disks.



ccrr003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

HP-UX HotPlug Disk Drive Replacement

The internal disk drives (two) are located at the front left side of the server (behind the bezel). When proper software and hardware procedures are followed, internal disk drives can be removed and replaced while the server is running.

NOTE MPE/iX does not support hotplug. Do not use these procedures on HP e3000 servers.

The procedures in this section are in two parts: physically replacing the device in the server and performing the HotPlug software procedure.

The replacement disk drive must be the same product ID as the disk drive that is being replaced.

HotPlug Hardware Procedure

Be sure that all the software procedures in the Disk Drive Removal section have been performed prior to starting these steps.

To install a disk drive from the server, perform the following steps:

Step 1. Remove the front bezel.

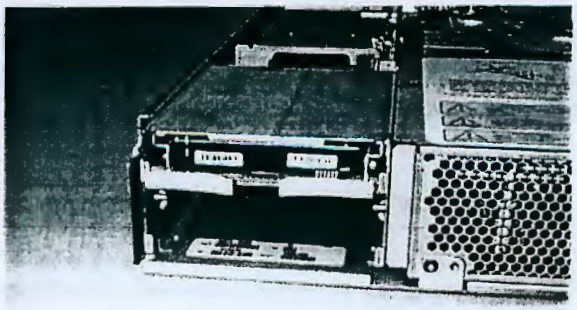
Step 2. On the left side of the front of the server you will see a door with a spring-loaded latch holding it shut. Open the door to expose the disk drive slots.

Step 3. Align the drive and carefully slide it completely into the selected slot with the extraction levers out.

Step 4. Fold the extraction levers in to engage and lock the disk drive in place.

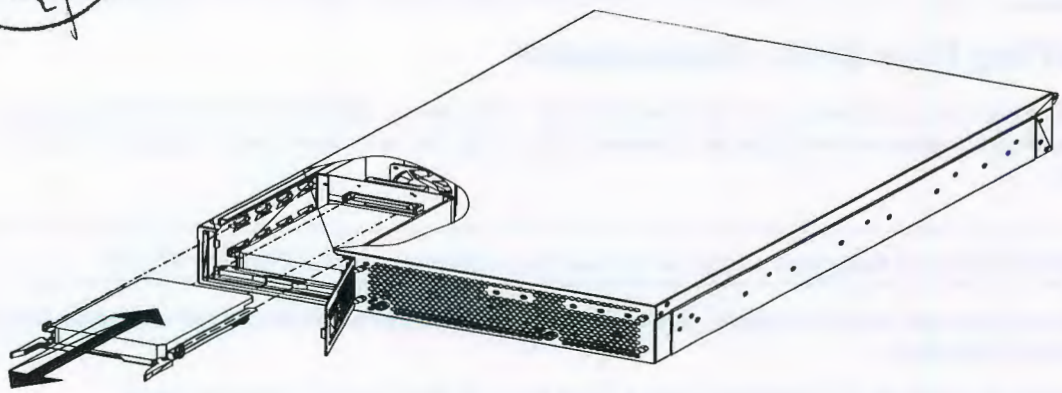
Step 5. Close the door and engage the spring-loaded latch to keep it shut.

The following photograph shows a HotPlug disk installed in the disk housing.



RQS nº 03/2005 - CN
CPMI - CORREIOS
243
Fls. Nº
3698
Doc.

The following graphic shows the location of the HotPlug disks.



ccrr003

HP-UX HotPlug Software Procedure

NOTE The HP-UX HotPlug software procedures for Disk Drive removal/replacement described below are for a mirrored boot disk configuration only. If your configuration differs from this, these procedures may not be valid. Consult your System Administrator or contact the HP Response Center for assistance.

HP-UX HotPlug Software Procedure for Attached Physical Volumes

Follow this procedure if the disk that was removed was recognized as an attached physical volume.

NOTE HP often uses different manufacturers for disks having the same product number. The HotPlug manual procedure will not update the disk drivers internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed) and also as a double check that it is a proper replacement and the device files are present. Refer to the above note. For example:

```
# ioscan -fnC disk
```

Step 2. Mirror the root disk:

a. Create the new physical volume using the *pvcreate* command. For example:

```
#pvcreate -B /dev/rdsk/cXtXdX
```

b. Extend the volume group to include the new physical volume using the *vgextend* command. For example:

```
#vgextend /dev/vg00 /dev/dsk/cXtXdX
```

c. Run the *mkboot* command to make the device bootable. For example:

```
#mkboot /dev/rdsk/cXtXdX
```

d. Use the *mkboot* command again to add the HP-UX auto-file-string. For example:

```
#mkboot -a "hpux" /dev/rdsk/cXtXdX
```

e. Run *lvlnboot*. For example:

```
#lvlnboot -R
```

f. *lvextend* a mirror into the replaced disk drive. This may take several minutes because this function copies all the data from the original copy of the data to the mirrored extents. The logical volume(s) are still accessible for users' applications during operation of this command.

```
#lvextend -m 1 <LV name> /dev/dsk/cXtXdX
```

For example:

```
#lvextend -m 1 /dev/vg00/lvol4/dev/dsk/cXtXdX
#lvextend -m 1 /dev/vg00/lvol5/dev/dsk/cXtXdX
```

Repeat this procedure for each logical volume to be mirrored

Step 3. Verify that the mirror is bootable and AUTO file is correct.

```
#lifls -l /dev/rdsk/cXtXdX
#lifcp /dev/rdsk/cXtXdX:AUTO -
```

Step 4. Verify that the mirroring is set up properly.

```
#vgdisplay -v /dev/vg00
#lvdisplay /dev/vg00/lol1 - lvol8
#lvlnboot -v /dev/vg00
```

Both disks should list as "Boot Disk" and both should appear in the *lvol* lists.

At this point, the system is fully functional.

HP-UX HotPlug Procedure for Unattached Physical Volumes

Follow these steps to replace a HotPlug disk drive for unattached physical volumes.

NOTE HP often uses different manufacturers for disks having the same product number. The HotPlug manual procedure will not update the disk drivers internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed) to verify that it is a proper replacement and the device files are present. Refer to the above note. For example:

```
# ioscan -fnC disk
```

Step 2. Restore the LVM configuration/headers onto the replaced disk drive from your backup of the LVM configuration:

```
#vgcfgrestore -n <volume group name> /dev/rdsk/cXtXdX
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 500
3698
Doc.

For example:

```
#vgcfgrestore -n /dev/vg00 /dev/rdsk/c2t4d0
```

Step 3. Attach the new disk drive to the active volume group with the *vgchange* command.

```
# vgchange -A y <volume group name>
```

For example:

```
# vgchange -A y /dev/vg00
```

Step 4. Run the *mkboot* command to make the device bootable. For example:

```
#mkboot /dev/rdsk/cXtXdX
```

Step 5. Use the *mkboot* command again to add the HP-UX auto-file string. For example:

```
#mkboot -a "hpux" /dev/rdsk/cXtXdX
```

Step 6. Run *lvlnboot*:

```
#lvlnboot -R
```

Step 7. Resynchronize the mirrors of the replaced disk drive. This may take several minutes since it has to copy all the data from the original copy of the data to the mirrored extents. The logical volume(s) are still accessible for users' applications during operation of this command.

```
#vgsync <VG name>
```

For example:

```
#vgsync /dev/vg00
```

The system is now functional.

I/O Card Cage Removal

The I/O Card Cage is located at the rear left side of the rp24xx server. To remove the I/O Card Cage, follow the steps listed below:

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

Step 1. On the rear bulkhead, remove cables attached to I/O card slots 2 through 4, located inside the card cage. Remove the cable attached to I/O card slot 1, located outside the card cage.

Step 2. Within the chassis, remove the I/O card from slot 1 on the right side of the I/O Card Cage, attached to the I/O Backplane as follows: If the card in slot 1 is a Secure Web Console card, unplug the 5V power connector from the receptacle on the card.

a. Remove the screw that attaches the I/O card to the rear bulkhead.

NOTE A short-shaft or right-angle Phillips-head screwdriver must be used to remove the screw due to the short distance between the screw head and the right side of the chassis.

b. Pull the I/O Card out of its slot on the I/O Backplane and place it on a clean anti-static surface.

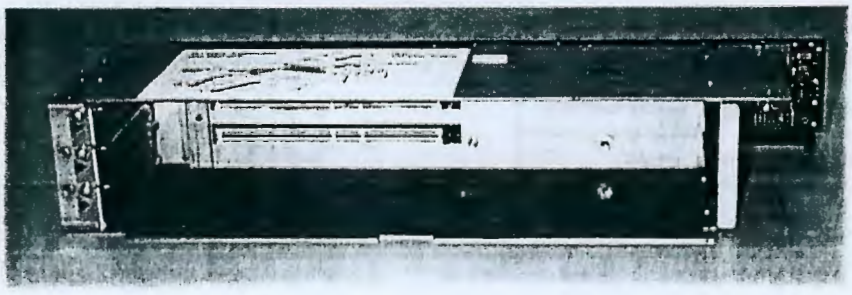
Step 3. Loosen the two captive Phillips-head screws located at the front of the Card Cage.

Step 4. Grasp the flat lever handle on the right side of the Card Cage and pull it up and forward to release the I/O Backplane from the System Board.

Step 5. Grasp the I/O Card Cage, tilt the front up, and pull it up and out of the chassis.

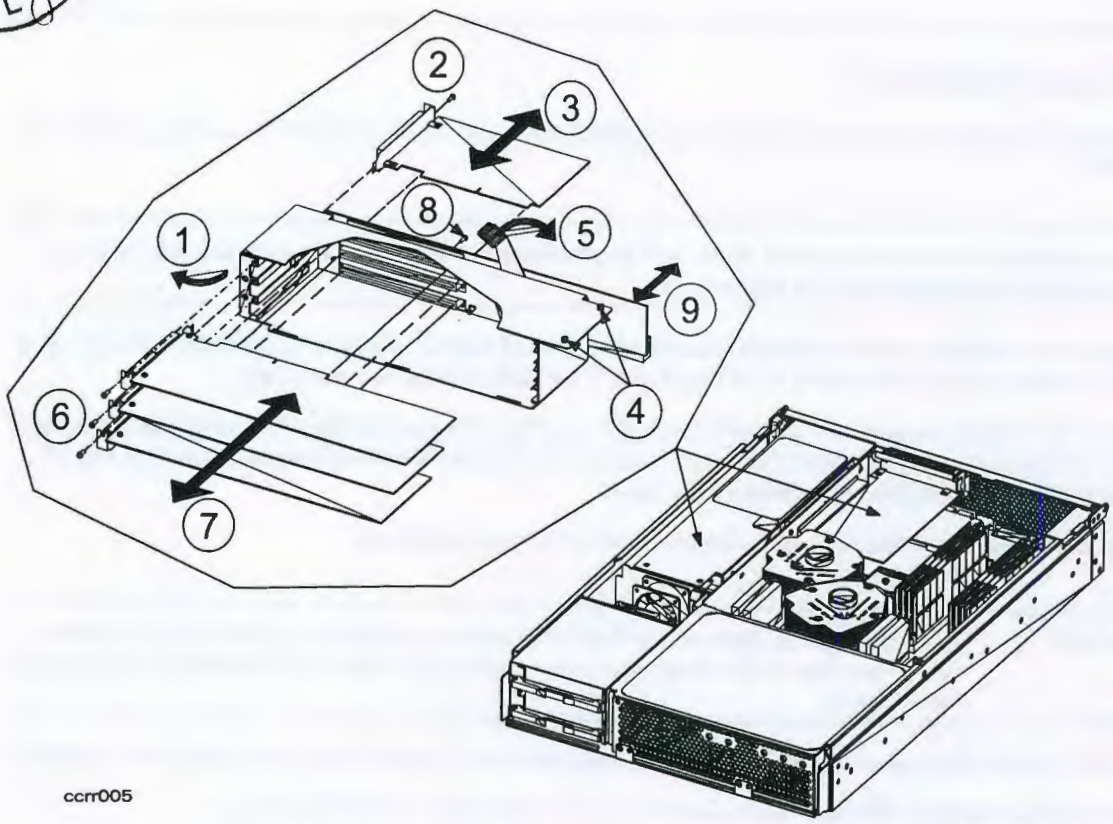
CAUTION Do not scrape the I/O Backplane against the CPU heat sink when you lift the card cage out of the chassis.

The following photograph shows an empty I/O Card Cage.



The following graphic shows an I/O Card Cage.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 561
Doc.



ccrr005

No.	Title
1	I/O Card Cage
2	I/O Card #1 slot tab
3	I/O Card #1 (short card only)
4	Top front captive screws
5	Flat lever handle
6	I/O Cards #2 through 4 slot tabs
7	I/O Cards #2 through 4 (long or short cards)
8	I/O Backplane retainer screw
9	I/O Backplane

I/O Card Cage Replacement

The I/O Card Cage is located at the rear left side of the rp24xx server. To replace the I/O Card Cage, follow the steps listed below:

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

Step 1. Grasp the I/O Card Cage, tilt the front up, and slide it down and into the chassis.

CAUTION To prevent damage to the I/O Backplane when removing or replacing the card cage, do not scrape it against the CPU heat sink as you move the card cage into or out of the chassis.

Step 2. Grasp the flat lever handle on the right side of the Card Cage and pull it up and out of the way. Align the I/O Backplane card connector with the System Board receiver and push in firmly to seat it. Push the flat lever handle down flush with the top of the Card Cage.

Step 3. Secure the two captive Phillips-head screws located at the front of the Card Cage.

Step 4. Replace the I/O card attached to the right side of the I/O Card Cage (slot 1) on the I/O Backplane as follows:

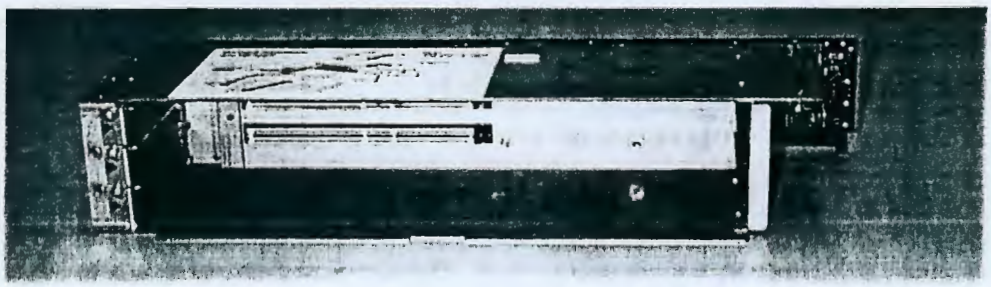
a. Seat the I/O Card into its slot on the I/O Backplane.

b. Replace the screw that attaches the I/O card to the rear bulkhead.

NOTE A short-shaft or right-angle Phillips-head screwdriver must be used to replace the screw due to the short distance between the screw head and the right side of the chassis.

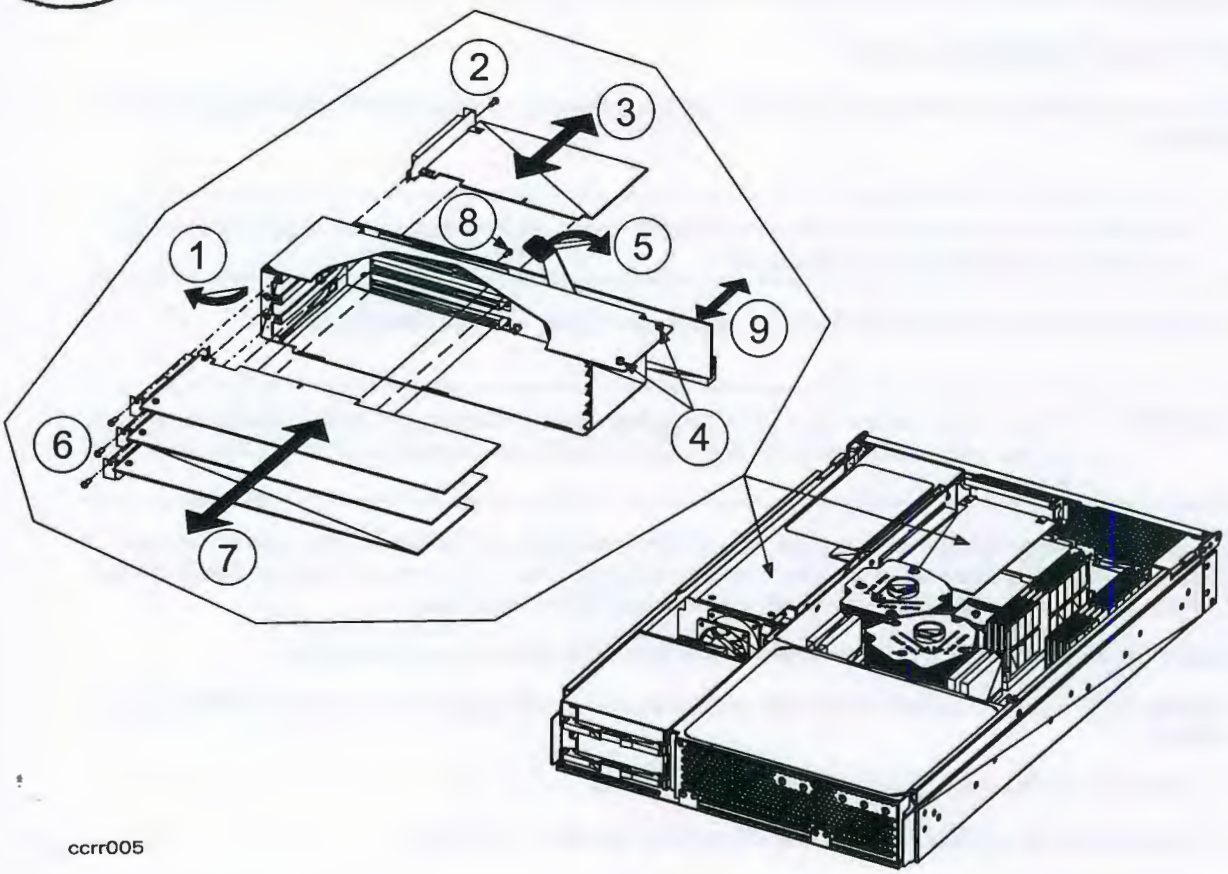
c. If the card in slot 1 is a Secure Web Console card, plug the 5V power connector into the receptacle on the Guardian Service Protector card.

The following photograph shows an empty I/O Card Cage.



The following graphic shows the components of an I/O Card Cage.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 249
Doc.



ccrr005

No.	Title
1	I/O Card Cage
2	I/O Card #1 slot tab
3	I/O Card #1 (short card only)
4	Top front captive screws
5	Flat lever handle
6	I/O Cards #2 through 4 slot tabs
7	I/O Cards #2 through 4 (long or short cards)
8	I/O Backplane retainer screw
9	I/O Backplane

PCI I/O Card Removal

PCI slots 2, 3, and 4 are located in the I/O Card Cage, which must be taken out of the chassis prior to removing these cards. PCI slot 1 supports a short PCI I/O card attached to the I/O Backplane and is located outside of the card cage If a Secure Web Console card was ordered as part of the system, it may be located in this slot and must be removed before taking the I/O Card Cage out of the chassis.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component. Always use an antistatic wrist strap and mat when working on the server.

Remove PCI I/O cards as follows:

- To remove PCI I/O card 1:
  a. Remove the screw that fastens the connector to the inside bulkhead.
  b. Pull the I/O card out of its slot on the outside I/O Backplane.

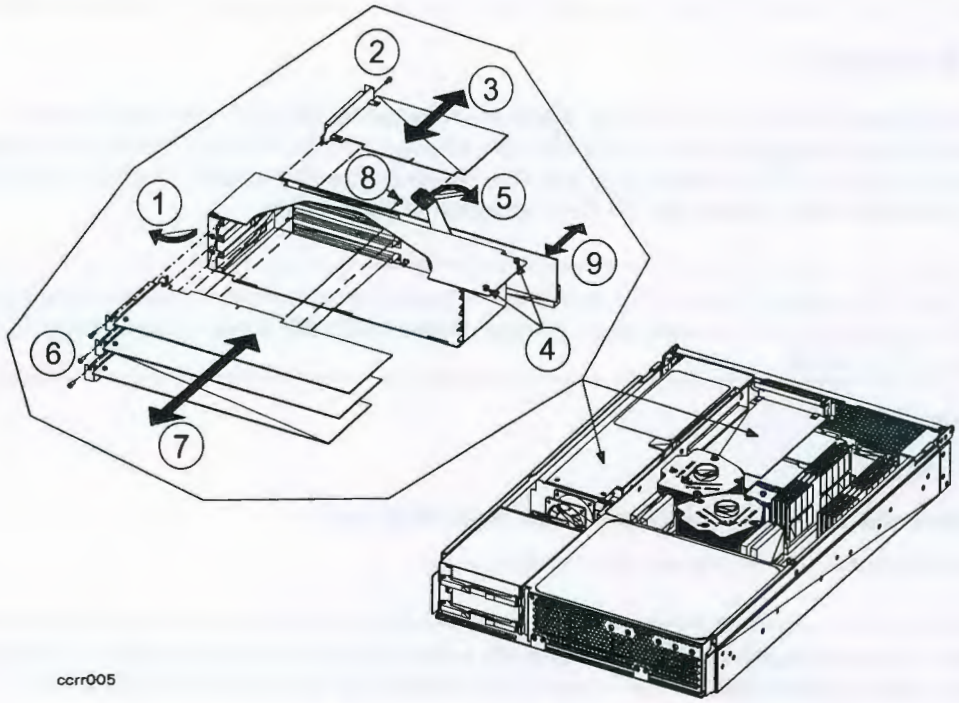
NOTE If you are removing the Secure Web Console card in the slot 1 position, ensure that the 5v power plug is removed from the power outlet (located on the Guardian Service Processor (GSP), front right side).

- To remove PCI I/O cards 2, 3, and 4:
  a. Take the I/O card cage out of the server.
  b. Grasp the edge of the I/O card and pull it out of its slot in the card cage.

The following graphic shows an exploded view of the I/O card cage with I/O cards.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 363
Doc. 3698

PCI I/O Card Removal



No.	Title
1	I/O Card Cage
2	I/O Card #1 slot tab
3	I/O Card #1 (short card only)
4	Top front captive screws
5	Flat lever handle
6	I/O Cards #2 through 4 slot tabs
7	I/O Cards #2 through 4 (long or short cards)
8	I/O Backplane retainer screw
9	I/O Backplane

PCI I/O Card Replacement

PCI slots 2, 3, and 4 are located in the I/O Card Cage, which must be taken out of the chassis prior to replacing these cards. PCI slot 1 supports a short PCI I/O card attached to the I/O Backplane and is located outside of the card cage. If a Secure Web Console card was ordered as part of the system, it may be located in this slot and must be replaced after reinstalling the I/O Card Cage in the chassis.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component. Always use both an ESD antistatic wrist strap and and ESD mat when working on the server.

To replace PCI I/O cards, proceed as follows:

- To replace PCI I/O cards 2, 3, and 4:

NOTE If a PCI card is installed in slot #1 (outside of the I/O card cage), it must be removed before the card cage can be removed from the server.

a. Take the I/O card cage out of the server.

b. Orient the replacement I/O card in its guide slot and push it into the card cage until the card connector seats in the I/O Backplane.

c. Replace the screw that fastens the I/O connector to the bulkhead.

- To replace PCI I/O card 1:

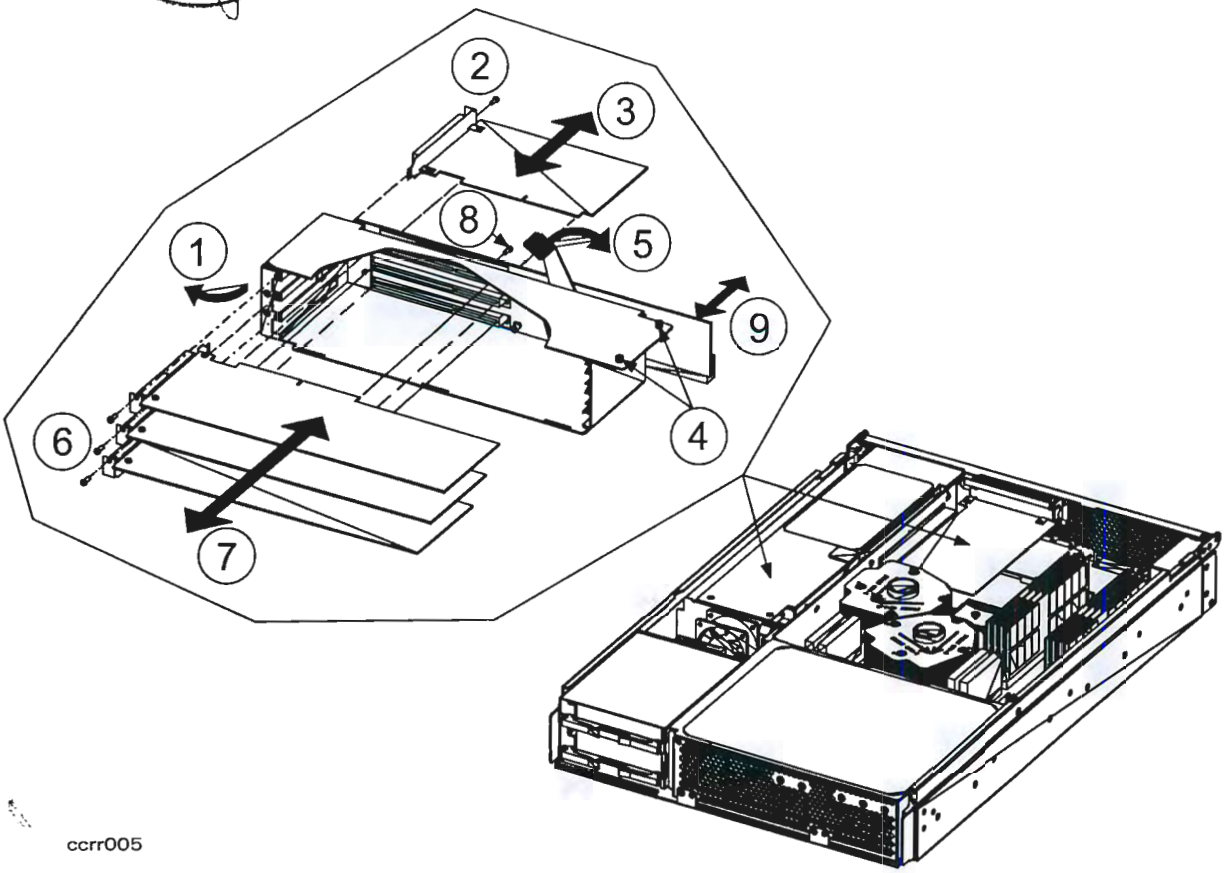
a. Push the I/O card into its slot until the card connector seats in the outside I/O Backplane.

b. Replace the screw that fastens the connector to the inside bulkhead.

NOTE If you are replacing the Secure Web Console card, ensure that the 5v power plug is seated into power outlet (located on the Guardian Service Processor, front right side) after the card is installed.

The following graphic shows an exploded view of the I/O card cage with I/O cards.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 564
3698
Doc.



ccrr005

No.	Name	No.	Name
1	I/O Card Cage	6	I/O Card anchor screws
2	Outside I/O Card anchor screw	7	I/O Cards #2 through #4
3	Short I/O Card #1 (may be Secure Web Console)	8	I/O Backplane anchor screw
4	I/O Card Cage anchor quarter-turn fasteners	9	I/O Backplane
5	I/O Backplane disconnect lever		

PCI Backplane Removal

The PCI backplane is located on the back of the I/O Card cage. I/O slot 1 is located on the outside of the PCI I/O card cage and slots 2, 3, and 4 are attached to the PCI backplane inside the I/O card cage.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To remove the PCI backplane from the server, perform the following steps:

Step 1. Remove the I/O cables from the back of the server.

Step 2. Remove the I/O card from slot 1.

Step 3. Remove the I/O card cage from the server.

CAUTION Do not scrape the I/O Backplane against the CPU heat sink when removing or replacing the card cage. Failure to heed this precaution could cause serious damage to the backplane and require replacement.

Step 4. Remove all PCI cards.

NOTE Note the order of PCI card installation prior to removal. Cards must be re-installed in the same slots, or I/O reconfiguration may be required.

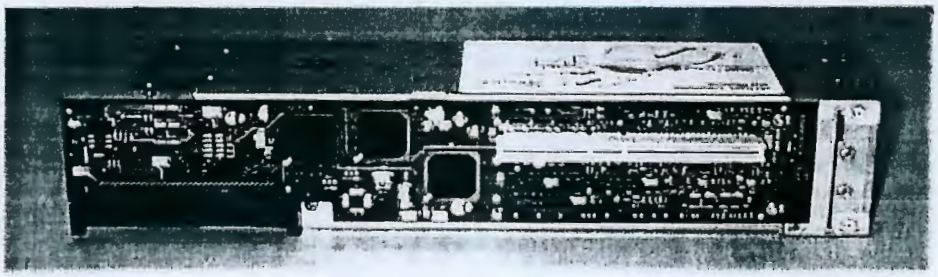
Step 5. Lay the I/O card cage, open side down, on a clean, dry surface. The PCI backplane is facing up.

Step 6. Remove the T-10 retainer screw from the PCI backplane.

Step 7. Slide the PCI backplane to one side, so that the retainer posts will clear the keyhole slots.

Step 8. Grasp the PCI backplane by the edges and carefully remove it from the card cage.

The following photograph shows the PCI Backplane.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 255
Doc. 3698

PCI Backplane Replacement

The PCI backplane is located on the back of the I/O Card cage. I/O slot 1 is located on the outside of the PCI I/O card cage and slots 2, 3, and 4 are attached to the PCI backplane inside the I/O card cage.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To replace the PCI backplane, perform the following steps:

Step 1. Lay the I/O card cage, open side down, on a clean, dry surface. When installed, the PCI backplane will be facing up.

Step 2. Grasp the PCI backplane by the edges and carefully set it on the card cage retainer posts.

Step 3. Slide the PCI backplane to one side so that the retainer posts lock into the keyhole slots.

Step 4. Replace the T-10 retainer screw that secures the PCI backplane to the card cage.

Step 5. Replace all PCI cards.

NOTE PCI Cards must be re-installed in the same slots from which removed, or I/O reconfiguration may be required.

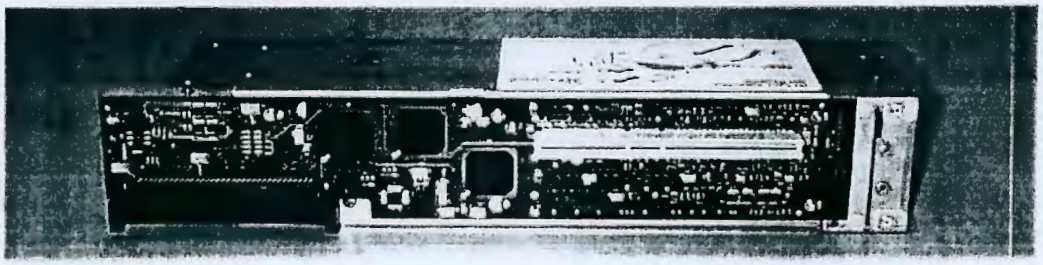
Step 6. Replace the I/O card cage into the server.

CAUTION Do not scrape the I/O Backplane against the CPU heat sink when removing or replacing the card cage. Failure to heed this precaution may cause serious damage to the backplane.

Step 7. Replace the I/O card in slot 1.

Step 8. Attach the I/O cables to the back of the server.

The following graphic shows the PCI Backplane.



RQS nº 03/2005 - CN
CPMI - CORREIOS
257
Fls. Nº
Doc.

DC-DC Converter Removal

DC-DC Converter boards and slave boards are required to power each CPU.

CPU MHz	Master	Slave
440	1	1
550*	1	2
* When available		

NOTE Each CPU requires a DC-DC Converter and slave(s) to operate. When upgrades are performed on the CPU, change the accompanying DC-DC Converter and slave(s) also. When returning replaced CPUs, return the accompanying DC-DC Converter and slave(s) also.

The converter boards stand on edge in slots and are located immediately behind the Power Supply on the left and right sides of the System Board, next to the CPU assemblies.

CAUTION DC-DC converter boards are not "hot-swap" or "hot-plug" units. Shut the server down and unplug the electrical connection prior to removing or replacing DC-DC converter boards.

To remove a DC-DC Converter board and its slave(s) from the server, perform the following steps:

Step 1. Gently pull the left and right levers away from each side of the board approximately 0.635 cm (1/4 in.).

CAUTION DO NOT press hard on the left/right levers or they will break. The levers do not extract the board from its socket. They provide vertical stability, only.

Step 2. Grasp the board by the left and right edges.

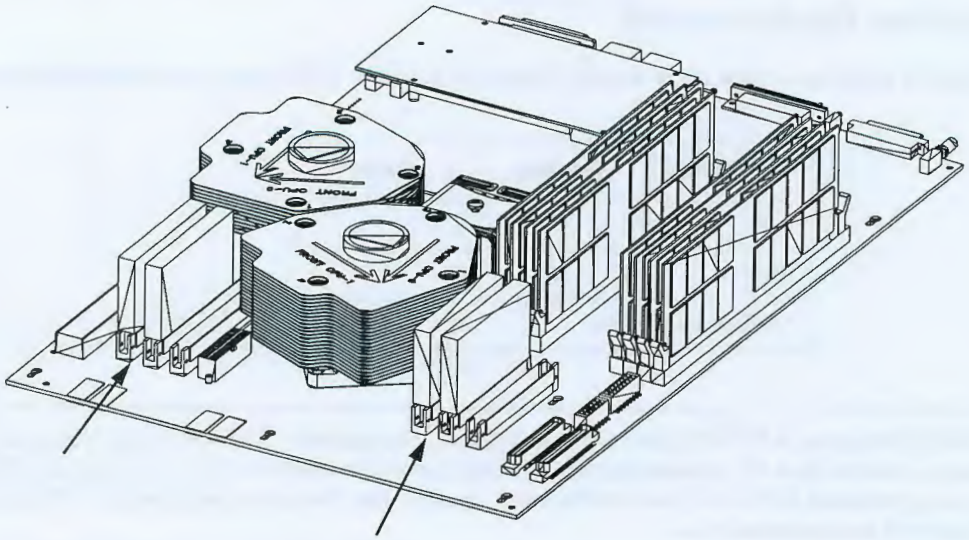
Step 3. With a gentle rocking motion, pull the board up and out of its slot.

Step 4. Place the board on a clean, static-free surface.

CAUTION There is little working room between the DC-DC converter boards and slave(s) and CPU-1. If necessary, use a flat-blade screw driver to reach and release the levers prior to removing these boards.

The following graphic shows the location of the DC-DC converter boards and slaves.

RQS nº 03/2005 - CN
CPMI - CORREIOS
271
Fls. Nº
Doc.



ccrr010

ROS nº 032005 - CN
CPMI CORREIOS
Fls. Nº
3698
Doc.

DC-DC Converter Replacement

DC-DC Converter boards and one or two slave boards (depending on the CPU speed) are required to power each CPU.

CPU MHz	Master	Slave
440	1	1
550*	1	2
* When available		

NOTE Each CPU requires a DC-DC Converter and slave(s) to operate. When CPUs are upgraded or replaced, ensure that the accompanying DC-DC Converter and slave(s) are changed. When returning replaced CPUs to Hewlett-Packard, ensure that the accompanying DC-DC Converter and slave(s) are returned also.

The converter boards stand on edge in slots and are located immediately behind the Power Supply on the left and right sides of the System Board, in front of the CPU assemblies.

CAUTION DC-DC converter boards are not "hot-swap" or "hot-plug" units. Shut the server down and unplug the electrical connection prior to removing or replacing DC-DC converter boards.

To replace a DC-DC Converter board and its slave(s) from the server, perform the following steps:

Step 1. Grasp the board by the left and right edges.

Step 2. Align the board connector with the slot. The slot and board are keyed so that the board will only fit one way. Place your thumbs on the top edge of the board, near the left and right sides, and push the board straight down into its slot until either an audible "click" is heard, or the levers close and seat into the slots in the side edges of the board

CAUTION DO NOT press hard on the left/right levers or they will break. Levers provide vertical stability, only.

The following graphic shows a DC-DC converter board and slave(s).

E C T
0180
C

DC-DC Converter Replacement

DC-DC Converter boards and one or two slave boards (depending on the CPU speed) are required to power each CPU.

CPU MHz	Master	Slave
440	1	1
550*	1	2
* When available		

NOTE Each CPU requires a DC-DC Converter and slave(s) to operate. When CPUs are upgraded or replaced, ensure that the accompanying DC-DC Converter and slave(s) are changed. When returning replaced CPUs to Hewlett-Packard, ensure that the accompanying DC-DC Converter and slave(s) are returned also.

The converter boards stand on edge in slots and are located immediately behind the Power Supply on the left and right sides of the System Board, in front of the CPU assemblies.

CAUTION DC-DC converter boards are not "hot-swap" or "hot-plug" units. Shut the server down and unplug the electrical connection prior to removing or replacing DC-DC converter boards.

To replace a DC-DC Converter board and its slave(s) from the server, perform the following steps:

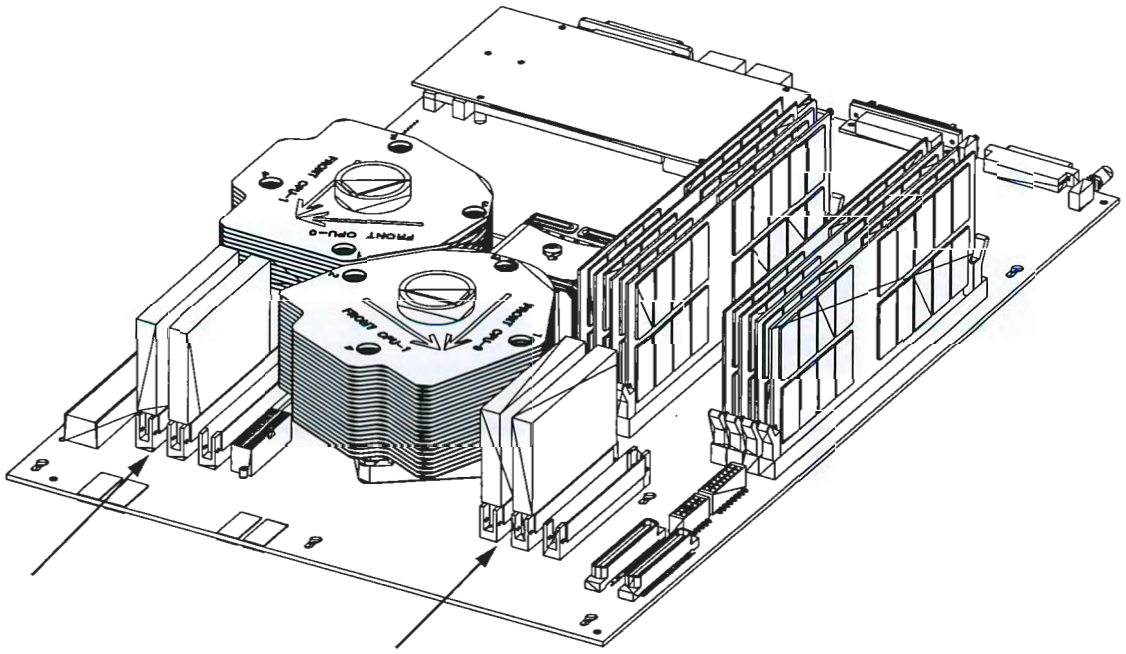
Step 1. Grasp the board by the left and right edges.

Step 2. Align the board connector with the slot. The slot and board are keyed so that the board will only fit one way. Place your thumbs on the top edge of the board, near the left and right sides, and push the board straight down into its slot until either an audible "click" is heard, or the levers close and seat into the slots in the side edges of the board

CAUTION DO NOT press hard on the left/right levers or they will break. Levers provide vertical stability, only.

The following graphic shows a DC-DC converter board and slave(s).

RQS nº 03/2005 - CO
CPMI - CORREIOS
Fls. Nº 569
3698
Doc.



ccrr010

Memory DIMM Removal

Memory DIMMs reside in eight sockets (two sets of four sockets each) located on the right side of the System Board. They are normally loaded in DIMM pairs of equal size.

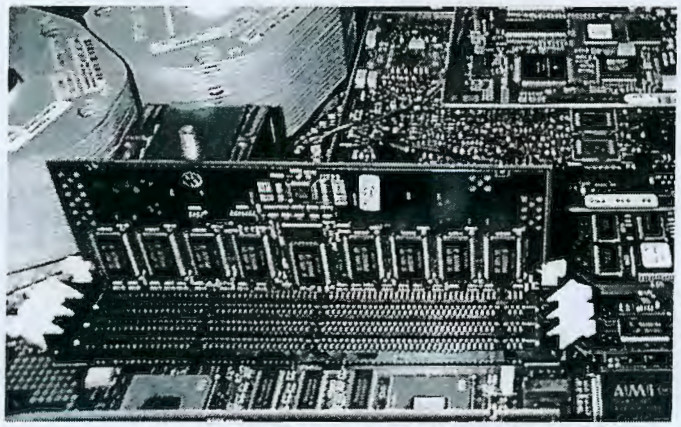
CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To remove a memory DIMM, perform the following steps:

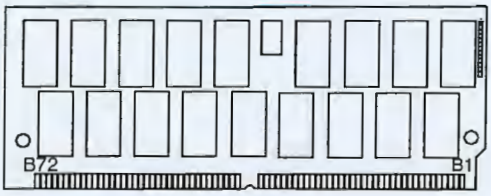
Step 1. Press down on the extractor levers on each end of the selected memory DIMM to unseat the DIMM from its socket.

Step 2. When the DIMM is unseated, pull it up and out of the System Board.

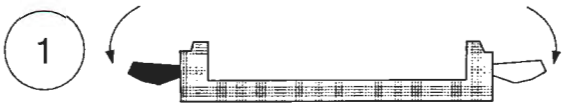
The following picture shows a memory DIMM located on the right side (from the server front) of the server system board.

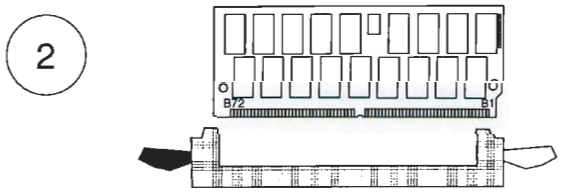


The next graphic is a drawing of a generic memory DIMM, followed by drawings that show DIMM removal/replacement.

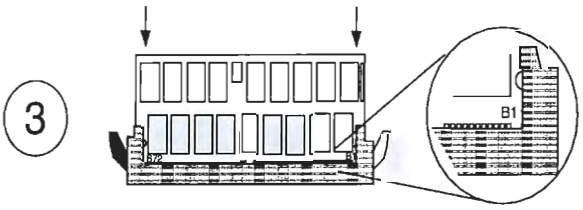


RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 570
Doc.





ulmu701



sun007

Memory DIMM Replacement

Memory DIMMs reside in sockets located on the right side (from the front) of the System Board.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

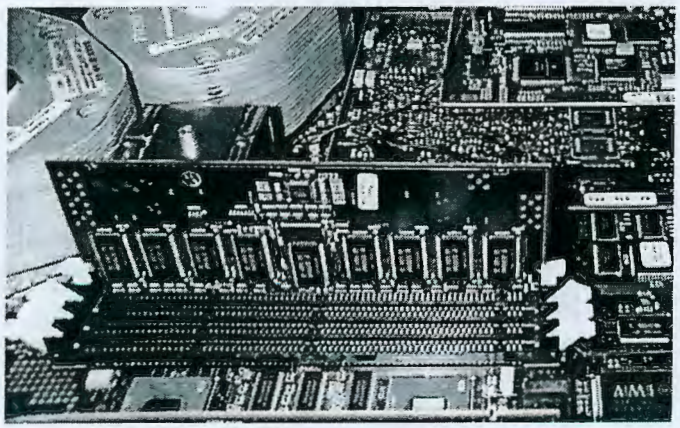
To replace a memory DIMM, perform the following steps:

CAUTION Be careful to insert the DIMM into the socket evenly. Do not rock the DIMM when seating it.

Step 1. Match the guide slots on the bottom of the DIMM with the guides on the socket and seat the memory DIMM into the socket. Insert the DIMM connectors into the guides until the card snaps firmly in place. It may be necessary to apply downward force using the palm of your hand on the DIMM. Ensure that one side the DIMM is not higher than the other.

Step 2. Use the BCH command `in me` to verify that the system recognizes the memory that you have just replaced.

The following picture shows the memory DIMMs located on the right side (from the server front) of the server system board.



The following graphic is a drawing of a generic memory DIMM, followed by drawings that show DIMM removal/replacement.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 571
Doc.

Guardian Service Processor (GSP) Removal

The GSP card resides on the System Board at the rear left center, under the short PCI I/O card (slot 1), which must be removed for access.

Before removing the GSP from the server, perform the following steps:

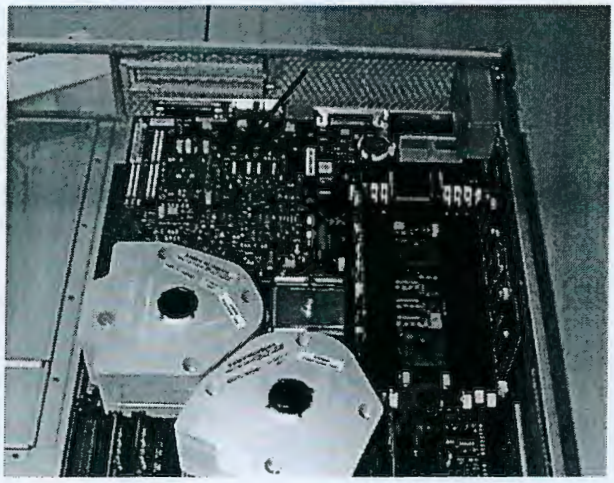
CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To remove the GSP from the server, perform the following steps:

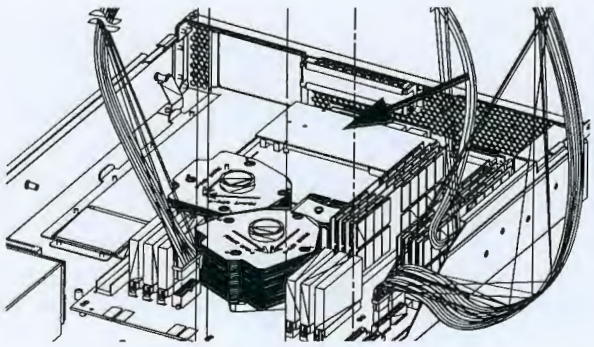
Step 1. Loosen the four mounting screws that hold the GSP card in place.

Step 2. Grasp the card by the left and right edges, rock it gently to free it from its socket on the System Board, and lift it out of the server.

The following picture shows the a GSP installed in a server.



The following graphic shows the location of a GSP in the server.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc.

Guardian Service Processor Replacement

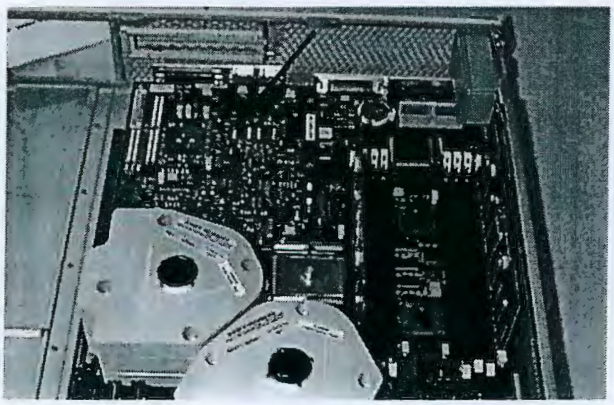
The GSP card resides on the System Board at the rear left center, under the short PCI I/O card (slot 1), which must be removed for access.

To replace the GSP, perform the following steps:

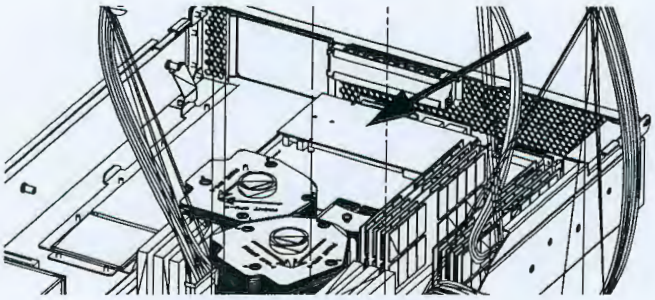
Step 1. Grasp the card by the left and right edges and press it gently into its socket on the System Board.

Step 2. Insert and tighten the four mounting screws that hold the GSP card in place.

The following picture shows a GSP installed in a server.

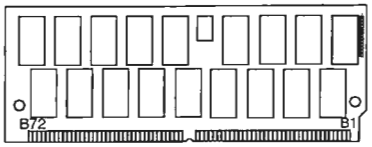


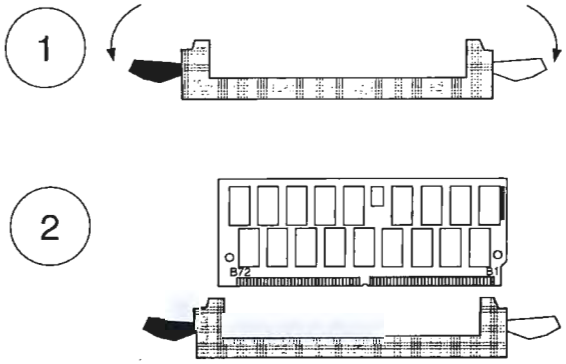
The following graphic shows the location of a GSP in the server.



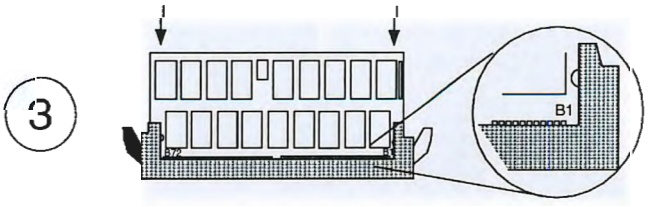
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 574
3698
Doc.





ulmu701



str007

Cisco Systems

Data Sheet

CiscoWorks **Campus Manager**

Campus Manager is a key component in the CiscoWorks family of management solutions designed to make Cisco networks the most manageable and available in the industry. Today's networks are critical business assets, and require sophisticated tools for administering, monitoring and configuring Layer 2 services. Designed for enterprise network operations staff, Campus Manager provides powerful tools with built-in network intelligence to reduce the complexity and automate manual tasks associated with maintaining complex physical and logical network infrastructures.

Campus Manager Overview

Campus networks are at the heart of business and mission-critical systems. The requirement to understand, monitor, and react to changing networking conditions drives the need for sophisticated, yet easy-to-use management tools. Campus Manager is part of the LAN Management Solution, part of the broad range of CiscoWorks network management solutions.

New in Version 3.3:

In addition to the rich set of management features already included, the new version of Campus Manager has been enhanced to provide even greater manageability for Cisco networks. New benefits include:

- Improved application performance
- Doubled capacity for tracking end users

Key Campus Manager features include:

- Intelligent discovery and display of Layer 2 networks on browser-accessible topology maps, independent of VTP server
- Configuration of virtual LAN (VLAN)/ LAN Emulation (LANE) and asynchronous transfer mode (ATM) services and assignment of switch ports to those services
- Link and device status display based upon Simple Network Management Protocol (SNMP) polling
- Identification of Layer 2 configuration discrepancies
- Diagnostic tools for connectivity related problems between end stations, and Layer 2 and Layer 3 devices
- Automatic location and correlation of information on users by media access control (MAC), IP address, NT or NetWare Directory Services (NDS) login or UNIX host name, with their physical connections to the switched network
- Visibility and launch point of Cisco CallManager from topology services as well as tracking of phone handset to IP, Mac address, and switch port
- Layer 2 and Layer 3 path trace between source and destination handsets
- Export of topology maps to Visio
- Java plugins to improve graphical user interface (GUI) performance

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Ability to form Custom Groups in Topology View based on criteria like SysLocation, SysName and IP address/ Subnet mask.

- Secure communication between the client browser and Campus applications using Secure Socket Layer (SSL) protocol.

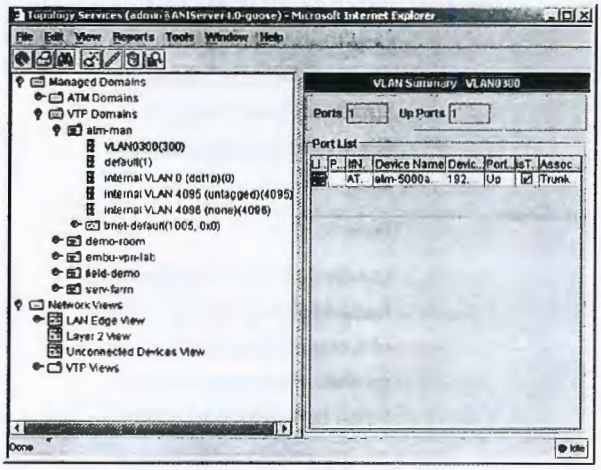
Campus Manager enables administrators to more easily change, monitor, and control network relationships, making them more effective in delivering business-critical and advanced networking services to their users and customers.

Campus Manager is a suite of applications launched from a common "management desktop" used by all Web-based CiscoWorks applications. Campus Manager contains three applications that can be launched from the client's browser:

- Topology Services—This is the principal interface to a variety of large scale topology maps, tabular summaries, reports, and configuration services of the Layer 2 network. A directory-like tree interface lists physical Layer 2 and logical, Virtual Trunking Protocol (VTP), and ATM domain views along with table summaries of the devices and interface associated with these views. This tree structure acts as the launching point for topology maps, discrepancy reporting functions, and configuration services. The integrated VLAN and LANE configuration capabilities, ATM soft permanent virtual circuit (PVC) configuration and diagnostic tools, along with physical and logical configuration discrepancy checking reports and highlighting tools are found within the Topology Services menus. It also supports discovery and display of Cisco Customer Response Applications, and reports on services of these devices.

  Ability to form custom groups based on dynamic and static rules for the group membership. System defined groups and user defined grouping can be created by network administrators and users respectively and allows grouping by developing rules based on criteria such as IP address, subnets, SysLocation, SysName, SysContact, Image Version and hostname. A rules editor allows for creating, editing Topology groups and defines rules for membership.

Figure 1
Topology Services Tabular View



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 2
VTP Domain Topology Map

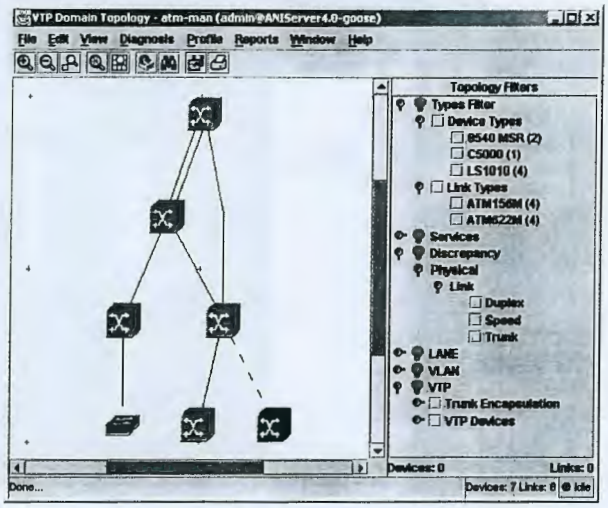
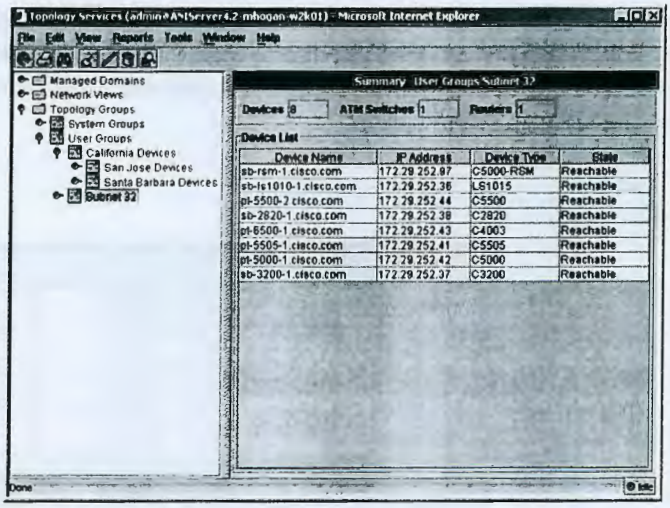


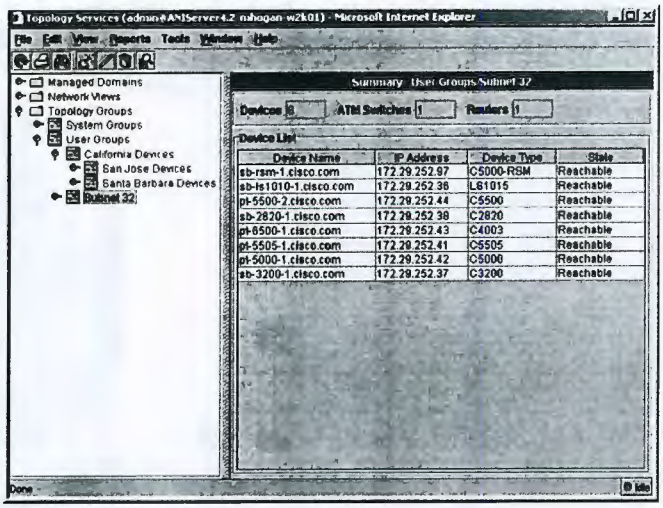
Figure 3
Forming Topology Groups



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

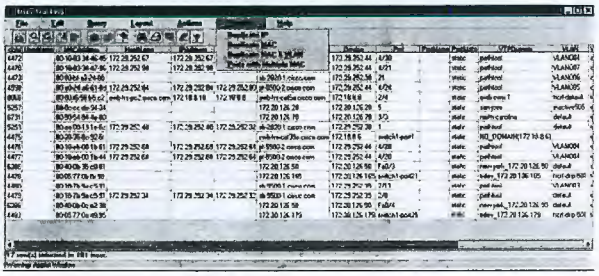
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 576
Doc.

Figure 4
Topology Group in Topology Maps



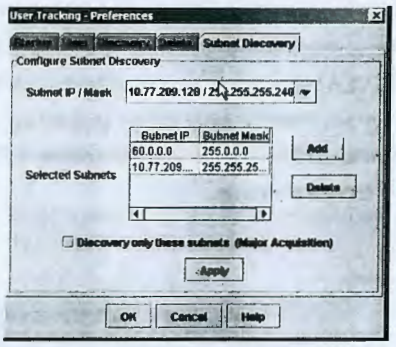
- User Tracking—Designed to assist in locating end-station connections at the access switch, this application is a useful tool in troubleshooting or connectivity analysis. Through automated acquisition, a table of end-user stations and Layer 2 connection information is constructed. This table can be sorted and queried allowing administrators to easily find users. Users can be identified by name, IP handset, MAC and IP address, as well as the switch port and switch that they are connected, along with VLAN and VTP assignment of the port. Predefined reports, such as duplicate MAC per switch port, or duplicate IP addresses, enable managers to locate mobile users or violations in port policies.

Figure 5
User Tracking



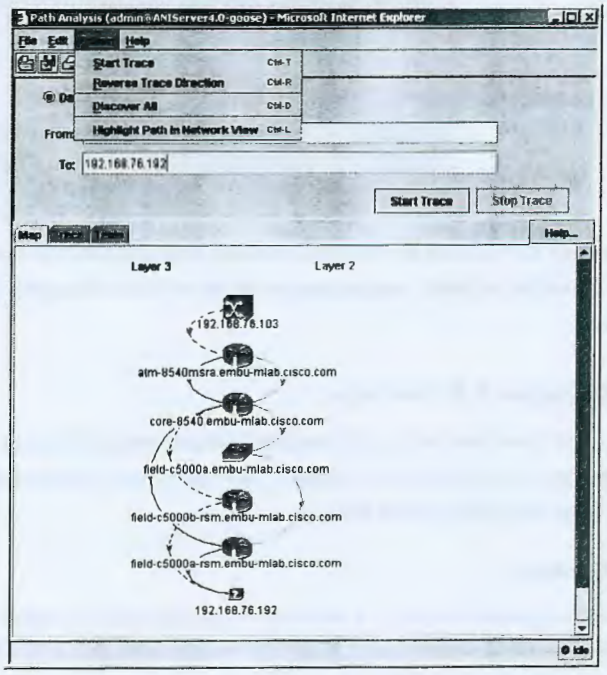
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 6
Subnet based acquisition



- Path Analysis—An application for switched network management, this is an extremely powerful tool for connectivity troubleshooting. Path Analysis utilizes User Tracking, topology services, and real-time spanning tree information to determine Layer 2 and Layer 3 connectivity between two end-points, or IP Handsets, in the network. The resulting trace is presented in graphical topology views that illustrate the Layer 2 and Layer 3 devices, path direction and link types, and in tabular formats that provide specific interface, IP address, VLAN, and link type information.

Figure 7
Path Analysis



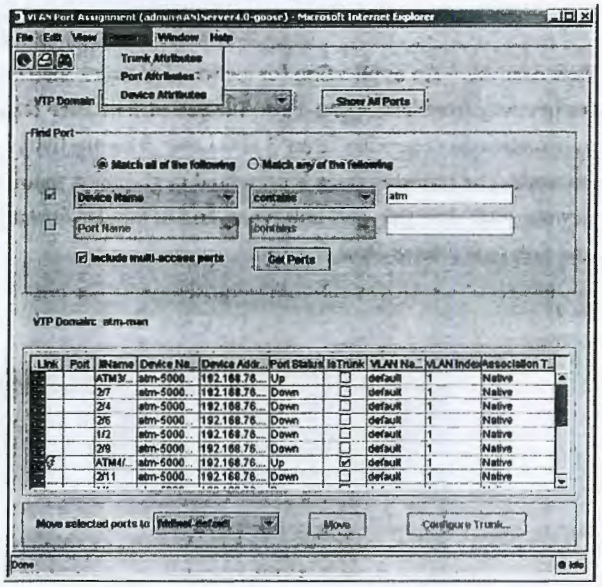
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

Figure 8
VLAN Port Assignment



Campus Manager 3.3 is a must for switched network management, and is an integral piece of the LAN Management Solution, by providing a broad, comprehensive set of tools for managing and administering the entire LAN environment.

Campus Manager 3.3 Features

Campus Manager provides a variety of functions within Topology Services, User Tracking, Path Analysis and VLAN/LANE port assignment that network managers can use to better understand, monitor, configure, diagnose, and be proactive to network infrastructure changes.

Topology Services

Topology Services provides access to a wide variety of physical and logical topology maps, summary lists of devices, ports, and their network relationships. Topology Services also acts as the launching point for topology-related configuration and diagnostic tools.

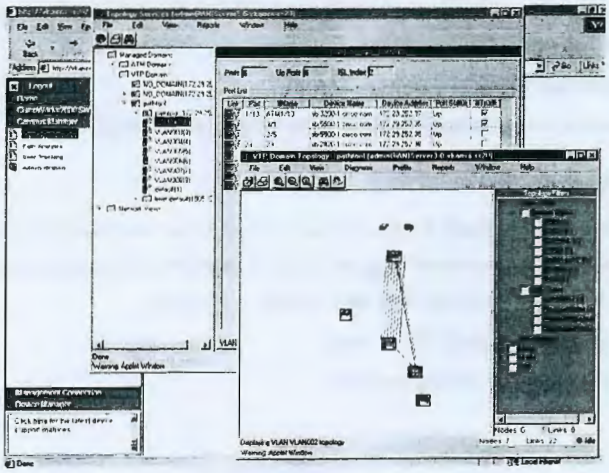
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

In Campus Manager 3.3, network topology maps can be displayed in a variety of ways from both a flat Layer 2 to abstracted views that better represent and scale to large campus networks. These abstractions are categorized into three different groups: managed domains, network views and topology groups. Managed domains are topological views of logical groups of devices organized around ATM switch fabrics and VTP domains. Network views are physical displays of the network and are organized to provide full and abstracted views, such as LAN edge views, Layer 2 views, unconnected device views, and VTP views. Topology Groups are custom views that are a subset of the entire network based on the group rule defined while creating the view. They are can be two types of groups—system defined groups that are custom views created by admin user and user defined views which are created by CiscoWorks users. Membership to these groups are made via rules that can be evaluated either automatically or upon user request and these groups help in generating custom views that are a subset of the Layer 2 views.

Key features in the Campus Manager topology services include:

- Autodiscovery and display of Cisco switches, routers, and probes using the Cisco Discovery Protocol (CDP) and SNMP
- Display of physical and logical Layer 2 connections within the discovered LAN environment
- Highlighting tools to identify specific classes of devices or links such as switches, route switch modules (RSMs), Fast Ethernet, EtherChannel®, ATM links, Cisco Customer Response Applications, and other relevant Cisco device elements
- Expanded scalability to support more than 2000 Cisco devices
- Display of multilayer switches and components (switching entities and route-processing entities) with the ability to highlight logical relationships between devices, such as flow masks and shortcuts
- Device status indicators on the topology maps based on CDP, ILMI, ELMI, and SNMP availability
- Automated discrepancy reporting during discovery highlights connection problems, link mismatches, and logical misconfigurations
- Graphical interface for creating VLAN and LANE services for Ethernet, Token Ring, and transparent VLANs
- Graphical interface for locating—through search parameters—and assigning switch ports individually or in bulk to a VLAN
- ATM soft PVC configuration and diagnostics

Figure 9
Topology Views and Tools



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 340
3698
Doc.

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

VLAN management services provide:

- Tabular summary views of VLANs shows participating ports, devices, links, and port status information
- Graphical setup of VLANs (including transparent VLANs) and VLAN membership to simplify administration
- Integration of LANE configuration services in VLAN configuration tools for more efficient operational and engineering practices
- A separate interface for administrators to quickly search, using a variety of criteria, and assign selected switch ports, individually or in bulk, to VLANs
- Logical display of VLAN configurations makes it easy to visualize switch connections
- Automated discrepancy reports highlight connection problems and link mismatches
- Automated VLAN membership registration reduces administration and configuration requirements

ATM Management

Campus Manager offers a graphical tool for managing complex ATM networks, simplifying configuration and performance monitoring. ATM networks are displayed on the topology map and the logical VLAN and ATM domain views provide graphical representations of ATM switches and LANE elements. "Drill down" capability allows access to configuration and performance monitoring tools. ATM management functions include:

- Autodiscovery of ATM switches, including switched virtual circuit (SVC) and PVC connections
- Connectivity checking of SVC and PVC connections
- End-to-end virtual circuit path tracing and analysis, which assists in connectivity diagnostics
- LANE troubleshooting and performance analysis
- Quality of service (QoS) templates for simplifying the configuration of typical traffic such as video or constant-bit-rate (CBR)
- Simple configuration of soft PVCs
- ATM remote monitoring (RMON) data collection and analysis

User Tracking

User Tracking automatically locates servers and end-user workstations, and Cisco voice over IP (VoIP) telephone handsets and their connections to Layer 2 Cisco switches. During this discovery process it also tabulates specific connection information about that end station, including:

- VLAN name, type, and VTP domain
- Switch port number, name, and state

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

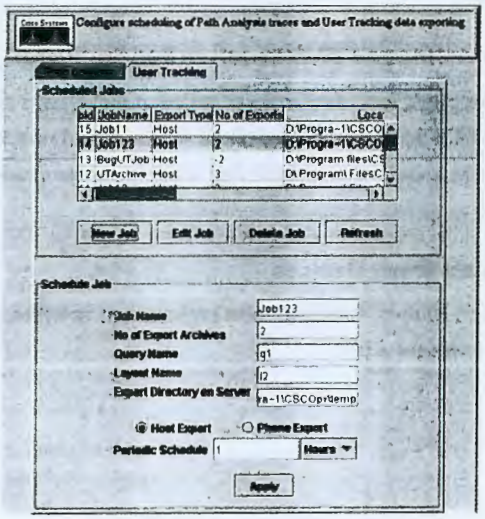
- MAC and IP address of the end station and its subnet
- Tabular and sortable listing of all switch port attached end-user workstations, servers and IP handsets
- Last-seen time stamp reflecting last acquisition in which the end station was detected
- User login name passed automatically from the Windows NT Primary Domain Controller or Novell Directory Structure, or from the UNIX host

Campus Manager simplifies the dynamic nature of many business environments by providing a large number of sortable parameters that can be used to locate end-user stations. User Tracking discovers end stations connected to switch ports automatically and provides a means to identify end users, their assigned VLANs, and host station connections. User Tracking also supports voice/data convergence with interfaces to Cisco CallManager for correlating the IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users.

User Tracking provides the following features:

- Enhanced scalability to support 60,000 end stations
- Predefined reports that identify duplicate MAC and IP addresses, ports with multiple MAC addresses and duplicate sysnames.
- IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users
- Tabular and sortable listing of all switch port-attached end-user workstations and IP handsets
- Customized tables for user-defined, detailed reporting
- GUI for user tracking information table configuration to support dynamic/mobile users
- Scheduling managers for automating address change updates
- Easy-to-use search utility box locating users by MAC addresses, IP addresses, DNS host names, switch port labels, and optional voice handsets
- Provides ability to schedule User Tracking. Also exports User Tracking reports.
- Ability to define acquisition based on a subnet range

Figure 10
Scheduled export of User Tracking Reports



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Path Analysis

Path Analysis is a powerful diagnostic tool for determining the Layer 2 and Layer 3 path between two selected endpoints using Campus Manager-discovered end-station data, VLAN/LANE configuration information, real-time Layer 3 path trace information, and spanning-tree calculations. Displays of path information are available in both topological map and tabular displays. Key Path Analysis features include:

- View the Layer 2 and Layer 3 path information in a map format with traces showing end stations, Layer 2 and 3 devices, route directions, and cut-through paths
- View specific details of the Layer 2 and Layer 3 path, including IP addresses and interfaces traveled, VLAN and VTP domain names, and port speeds and duplex settings
- Perform traces immediately or schedule them
- Perform traces using IP address, DNS name, or by telephone number for voice calls as start/stop points
- Provide Layer 2 and Layer 3 trace information between Cisco voice elements using interfaces to call detail records for specific voice calls
- Provides ability to schedule path traces. Also exports path traces data.

Built on the CiscoWorks Management Server

The CiscoWorks management server provides common resources, such as Web services, discovery, shared databases and database services, and the management desktop. Cisco Management Connection, a service on the CiscoWorks2000 server, delivers a set of tools for integrating applications into the management desktop using Internet-based standards and technologies. These tools allow users to link Web-based management applications to the CiscoWorks family of products and application developers to easily link Web-based applications through a certified registration mechanism. Cisco Management Connection has been used by Cisco and more than 30 network management vendors, including Hewlett-Packard, Computer Associates, Sun Microsystems, and Tivoli Systems to create certified Cisco Management Connections for their applications. This rapid adoption has created an environment in which users can easily build management intranets that link together their favorite Web-based management applications.

Specifications

Server, Client, and Web Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco Devices

Most Cisco routers, Catalyst® and LightStream switches, as well as Cisco AVVID devices. Contact your Cisco representative for a complete list.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Supported Cisco IOS Versions

- Cisco IOS® version 10.3 and above
- Catalyst Supervisor code 2.1 and above

Availability

Campus Manager 3.3 is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on Campus Manager, see:
http://cisco.com/warp/public/cc/pd/wr2k/

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

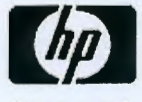
203048/ETMG_03/03

ECT
CPMI - CORREIOS
Fls. Nº 580
3698
Doc.

HP SureStore Disk System 2100

User's Guide

Edition E0301
Order No. A5675-90901
Printed in U.S.A.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 581
Doc. 3698

Notice

© Hewlett-Packard Company, 2000. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Warranty

If you have any questions about the warranty for this product, contact your dealer or local Hewlett-Packard sales representative.

Safety Notices

To protect against personal injury and product damage, do not attempt to lift the product without the assistance of another person or lift device.

Components bearing this symbol may be hot to touch.

Components bearing this symbol are fragile. Handle with care.

Components bearing this symbol are susceptible to damage by static electricity. ESD precautions are required.

Operation

The front door should be closed and locked at all times during the operation of this product except when replacing disks.

This product is intended to be operated in a restricted access area.

Service

Maintenance or repair of the backplane and mezzanine boards must be performed by authorized service-trained personnel.

Format Conventions

	Denotes
WARNING	**A hazard that can cause personal injury**
CAUTION	A hazard that can cause hardware or software damage
Note	Significant concepts or operating instructions
this font	Text to be typed verbatim: all commands, path names, and file names. Also menu and button selections in GUI contexts
`this font`	Text displayed on the screen

Components of the Disk System **12**
Front Panel 12
System Power LED 12
Rear Panel 13
SCSI ID Switch 14
Power Connector 15
Electrical Requirements **15**
AC Site Requirements 15
Installing the Disk System **16**
Hardware Requirements 16
Preparing for Installation 16
Setting the SCSI IDs for the Disk Modules 17
Installing the Disk System **18**
Connect the SCSI Cables 18
Connecting the Power Cable 20
Powering On and Off **20**
Power On the Disk System 20
Power Off the Disk System 21
Adding Disk Modules **22**
Add a Disk Module 22
Configure the new Disk Module 23
Remove and Replace A Disk Module **23**
Removing a Disk Module 23
Replace a Disk Module 24
Remove the Disk System **25**
Setting Up the Hardware Event Monitor (HP-UX Only) **26**
Configuration Overview **26**
Event Notification (HP-UX Only) 27
Status LEDs 29
View Disk Status **30**
STM Disk Information: HP-UX 30
STM Disk Information: MPE/iX 6.5 or 7.0 32
Isolating Faults 34
Reference Information **35**
Product Numbers and Options 35
Upgrade Disk Products Available 36
Specifications 38
Electrical Specifications 38
Operating Temperatures 39
Regulatory Statements **39**
Safety Certifications 39
EMC Compliance 39
A. FCC Notice for United States 40
B. FCC Notice for Canada 40

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 582
3698
Doc.

C. Notice for Japan 41
Harmonics Conformance (Japan) 41
D. Notice for Taiwan 41
E. Notice for Korea 41
F. Notice for Germany 41
Product Web Site 43
Related Documents 43

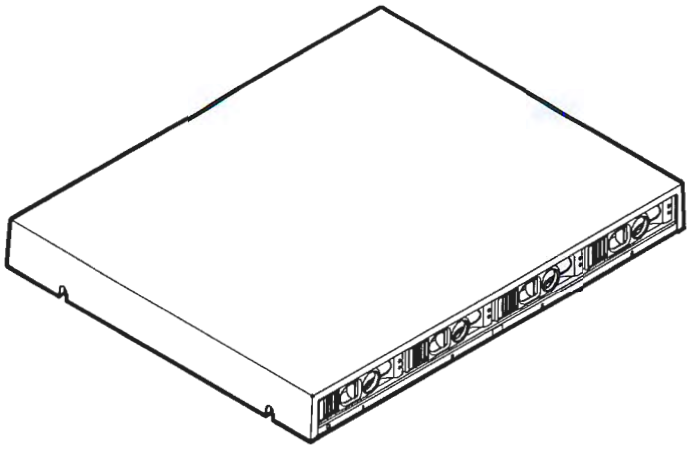
Figure 1. Disk Module LEDs. 12
Figure 2. Disk System Power LED 12
Figure 3. Rear View of the Disk System 13
Figure 4. Power Button 13
Figure 5. SCSI ID Switch Settings 14
Figure 6. AC Power Connector Location 15
Figure 7. SCSI Switch Location 17
Figure 8. SCSI Port Locations 18
Figure 9. AC Power Connector Location 20
Figure 10. Power Button Location 21
Figure 11. Installing a disk module 23
Figure 12. Removing the Disk System 25
Figure 13. Sample Hardware Event Notification 28
Figure 14. LED Status Indicators 29
Figure 15. Sample STM Information Log (HP-UX) 31
Figure 16. Sample STM Expert Tool Disk Error Log (MPE/iX 6.5 or 7.0) 33

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

Table 1 Disk LED Activity Defiinitions 12
Table 2 Disk System Power LED Activity Definitions 13
Table 3 AC Power Requirements 15
Table 4 SCSI Switch Setting Definitions 17
Table 5 SCSI Address Priority 18
Table 6 LED Status Indicators 29
Table 7 Troubleshooting Table 34
Table 8 Products and Options 35
Table 9 Available Upgrade Disk Modules 36
Table 10 Upgrade Products for Hewlett-Packard Systems 36
Table 11 Replaceable Parts 37
Table 12 Supported HP Cables and Terminators (for Enterprise Systems) 37
Table 13 Supported HP Cables and Terminators (for Commercial Systems) 38
Table 14 Physical Dimensions 38
Table 15 AC Power Requirements 38
Table 16 Environmental Specifications 39

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

The HP SureStore Disk System 2100 is a first-generation 1-EIA Unit disk system capable of accomodating up to four disk modules. It is designed to provide inexpensive, high performance rack-optimized online mass storage for entry-level configurations in three distinct markets: (1) HP servers/workstations, (2) open systems JBODs, and (3) open systems IDACs (Internal Disk Array Controller).



ECT AC

Components of the Disk System

Front Panel

The disk modules can be accessed from the front of the disk system. It can accept up to 4 low profile disk drives. If your storage system contains less than 4 disk modules, the remaining empty slots require filler panels. These filler panels (part number A6198-60001) ensure that the proper cooling is maintained within the storage system.

FIGURE 1 Disk Module LEDs

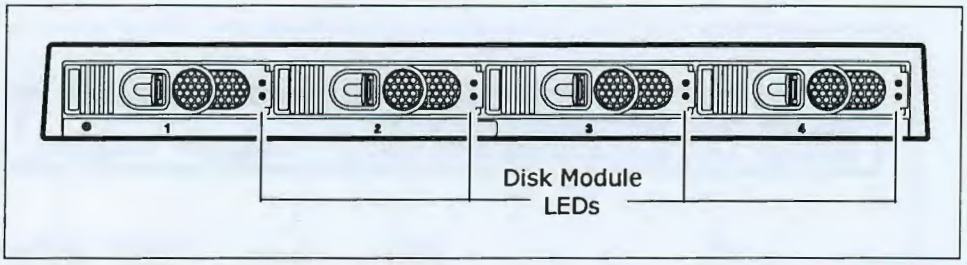


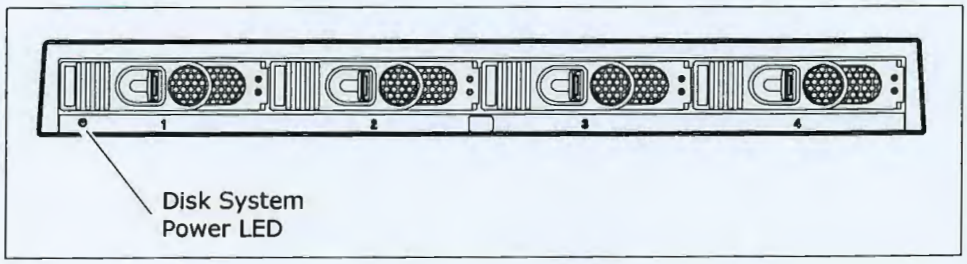
TABLE 1 Disk LED Activity Defiinitions

LED Activity	Indication
Blinking	Disk activity
All on solid for approximately1 second	Bus reset
Off	Disk is idle or off

System Power LED

The System Power LED gives diagnostic information about the disk system operation. Refer to Table 2 on page 10 for more information.

FIGURE 2 Disk System Power LED



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 585
Doc. 3698

TABLE 2 Disk System Power LED Activity Definitions

LED Activity	Indication
Blinking	Malfunction - either a fan is not operating properly or internal voltage is too low.
On solid	Disk system is operating properly.
Off	Disk system is off.

Rear Panel

FIGURE 3 Rear View of the Disk System

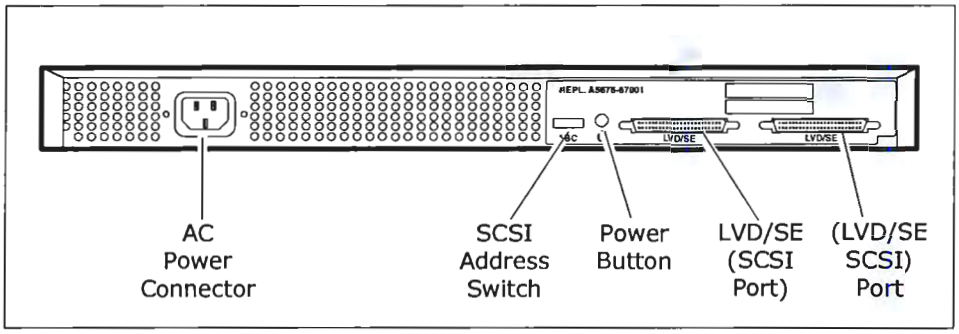
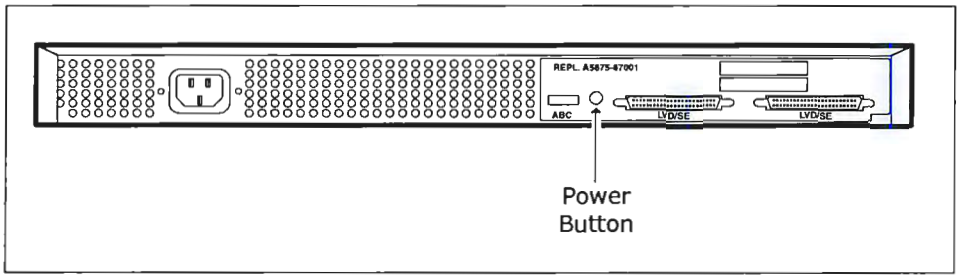


FIGURE 4 Power Button



With the power button in the "ON" position, power is supplied to the disk system.

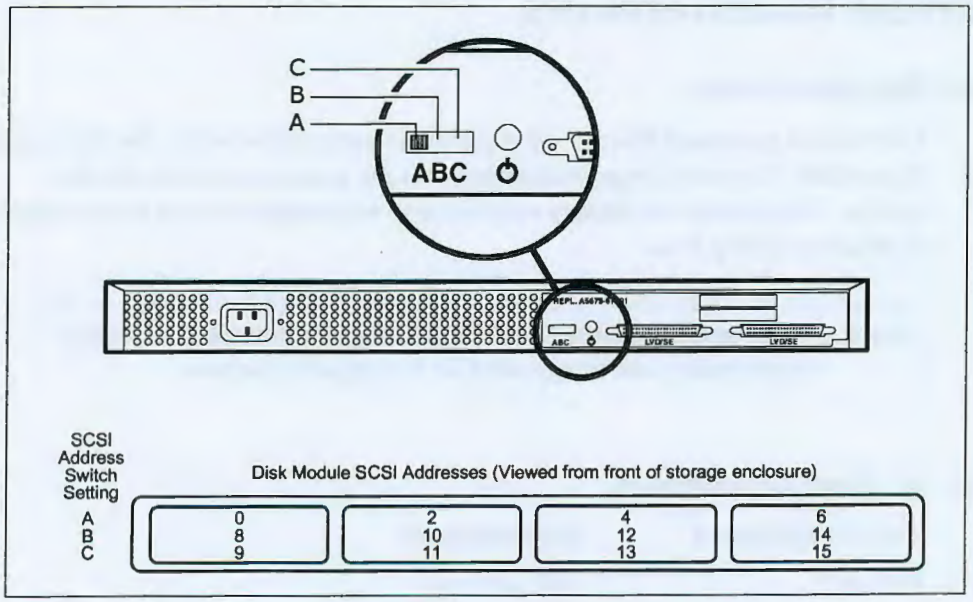
SCSI ID Switch

The SCSI ID switch sets the address for the disk drives.

There are three possible settings for the SCSI address switch: A, B, and C. Each setting assigns a different *set* of addresses to the disk modules installed in the disk system. For SCSI address switch setting A, the addresses for the installed disk modules are (from left to right, looking at the disk system from the front) 0, 2, 4, and 6. For SCSI address switch setting B, the addresses for the installed disk modules are 8, 10, 12, and 14. For SCSI address switch setting C, the addresses for the installed disk modules are 9, 11, 13, and 15. See Figure 5, below.

SCSI address 7 is reserved for use by the host bus adapter.

FIGURE 5 SCSI ID Switch Settings

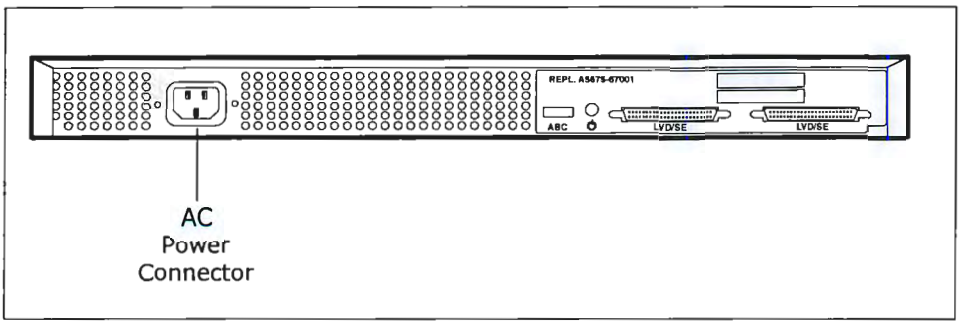


Note The disk system requires a terminator when it is installed at the end of the SCSI bus.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 536
Doc. 3698

Power Connector

FIGURE 6 AC Power Connector Location



Electrical Requirements

AC Site Requirements

Overcurrent protection devices are required for each cabinet where the disk system is installed. They must be positioned between the power source and the disk system. These protective devices must not trip when exposed to an inrush current of 30 amps lasting 5 ms.

> **Note** These protection devices must meet all applicable electrical safety requirements and be approved for the intended purpose.

TABLE 3 AC Power Requirements

Electrical Element	Requirements
Voltage	100-240 VAC
Frequency	50-60 Hz
Input current	< 1 amp
Maximum Surge Current	30 amps peak

E C T
CPL - AC

Installing the Disk System

Hardware Requirements

The following hardware is included with the disk system:

One power cord comes with each disk system.

Your host computer must have one of the following:

- An on board UltraSCSI port
- An UltraSCSI host adapter board installed in the host system:
  - A5149A Single Port Ultra 2 SCSI Host Bus Adapter (HP Series 9000 only)
  - A5150A Dual Port Ultra 2 SCSI Host Bus Adapter (HP Series 9000 only)
  - D5025A Ultrawide Host Bus Adapter for HP Netserver
  - D5955A Netraid 3si Host Bus Adapter for HP Netservers
  - D9161A Netraid 4M/64 Host Bus Adapter for HP Netservers
  - D9351A Netraid 4M/128 Host Bus Adapter for HP Netservers
  - P3413A Single Port Ultra 3 SCSI Host Bus Adapter for HP Netservers

The following accessories are available for your storage disk system:

- A5149A Single Port Ultra 2 SCSI Host Bus Adapter
- A5150A Dual Port Ultra 2 SCSI Host Bus Adapter
- C2364A High Density 68-pin Terminator for LVD or Single-Ended

For Ultra 3 SCSI performance, the host port or host adapter to which you connect your disk system must be Ultra 3 SCSI capable. If you connect your disk system to a SCSI narrow or wide adapter, the device performs at lower speeds. Also, if you connect the disk system to an UltraSCSI capable host bus adapter using a non-Ultra 3 SCSI cable, the data transfer rate will be lower.

Preparing for Installation

Before the disk system is ready for installation, its SCSI IDs must be set and the host system must be prepared to recognize the newly installed disk system. See your operating system administration manual for configuration procedures for the host bus adapter.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 587
Doc. 3690

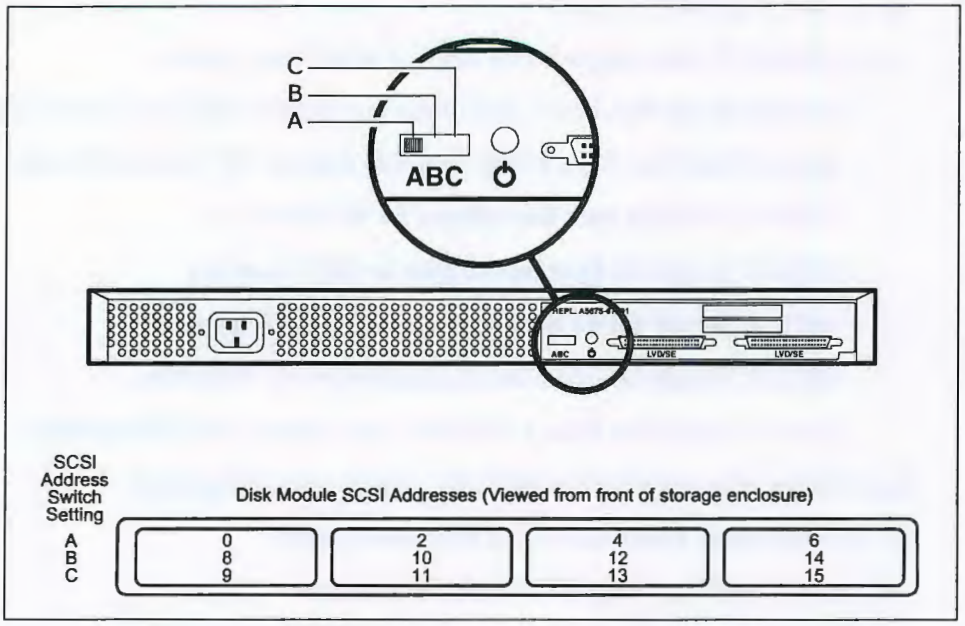
Setting the SCSI IDs for the Disk Modules

1 Determine which SCSI addresses are not being used on the host system.

Refer to your system administration manual for information on determining which SCSI addresses are available on the host system.

2 Locate the SCSI switch on the back of the disk system.

FIGURE 7 SCSI Switch Location



3 Set the SCSI IDs

Verify that the SCSI IDs you have chosen are available. If you are daisy-chaining these disk systems together, each one's SCSI ID switch must be set for a unique available set of SCSI IDs.

TABLE 4 SCSI Switch Setting Definitions

SCSI Switch Setting	Disk Slot			
	1	2	3	4
A	0	2	4	6
B	8	10	12	14
C	9	11	13	15

ECT - CPL - AC

Keep in mind that the host bus adapter should have the highest SCSI address priority. See Table 5 below.

TABLE 5 SCSI Address Priority

SCSI ID	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
Priority	Highest															Lowest

Installing the Disk System

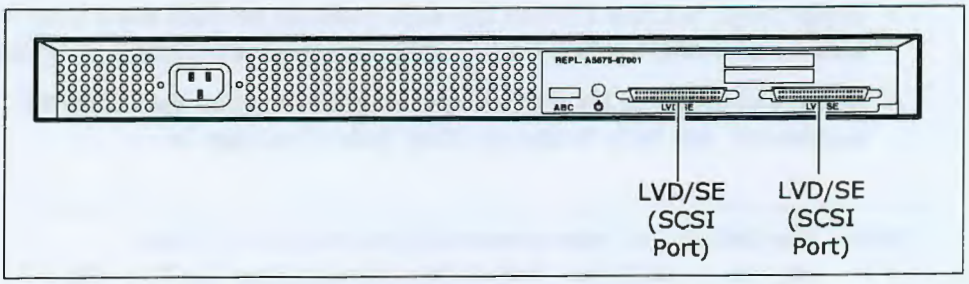
See the installation instructions enclosed with your rackmount kit.

Connect the SCSI Cables

1. Make sure that the host system has been powered down.
2. Connect one end of an ultra SCSI cable (get it from the shipping box) to the host system. To acheive Ultra 3 SCSI speeds, the host bus adapter, the SCSI cables, and the disks must be able to transmit data at UltraSCSI 3 speeds. For the SCSI port location on your host system, refer to your host system's documentation.

   You may connect non-Ultra 3 SCSI cables to the disk system, but the data transmission rates will be lower.
3. Connect the other end of the SCSI cable to one of the LVD/SE ports on the rear of the disk system.

FIGURE 8 SCSI Port Locations



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 588
3698
Doc.

4 Determine if this disk system is at the beginning or end of the SCSI bus.

- If the disk system is at the end of the SCSI bus (you are not going to daisy-chain another device off this one), install the appropriate terminator (part number 5183-2657) on the available SCSI port and go to "Connecting the Power Cable" (see Figure 9 on page 17).
- If the disk system is at the beginning or middle of the SCSI bus (you are going to daisy-chain another device off this one), consider the following:

  No more than 3 of these disk systems can be daisy-chained together.

  Ensure that the SCSI IDs assigned for the disk drives in the second disk system or other peripheral are not already assigned to another device on the SCSI bus. Refer to "Setting the SCSI IDs for the Disk Drives" (see Figure 7 on page 14 for the SCSI IDs assigned for each SCSI switch setting).

  If you connected the SCSI cable to the on-board UltraSCSI port on the host system, verify that the SCSI IDs assigned to the disk drives in the second disk system or additional peripherals are not already assigned to any other peripherals installed in the host system.

  The overall SCSI bus length cannot exceed 12 meters. The SCSI bus length for the disk system internal cables is 1.1 meters. If another type of peripheral is being connected on this SCSI bus, refer to that peripheral's documentation for its internal SCSI cable length.

5 Connect one end of an ultra SCSI cable (get it from the shipping box) to the available SCSI port on the rear of the first disk system on the SCSI bus.

6 Connect the other end of the ultrascsi cable to the SCSI IN port on the rear of the second disk system on the SCSI bus.

7 Repeat Steps 3, 5, and 6 for the last disk system on the SCSI bus if three disk systems are being installed. Keep in mind the maximum bus length (12 meters).

8 Install a terminator if the device is the last one on the bus. For supported terminators, see Table 10 on page 33 or Table 12 on page 34.

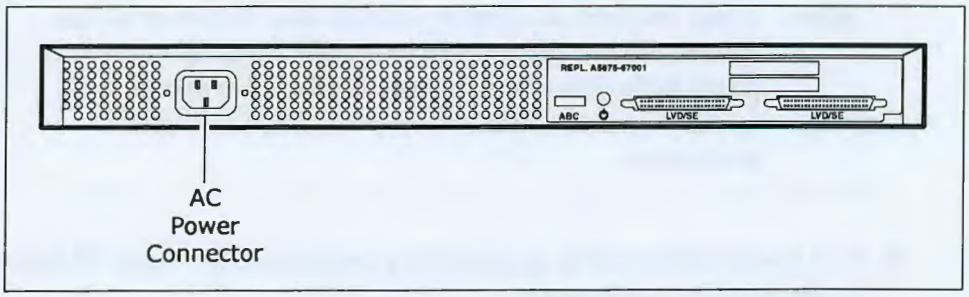
Note The disk system, when connected at the end of a SCSI bus, requires a terminator. Refer to the documentation that came with your wide SCSI device to determine if it needs a terminator or not. Narrow SCSI devices at the end of a daisy-chain always require a terminator.

ECT
CPL
AC

Connecting the Power Cable

CAUTION **Ensure that the connection of multiple units to the supply circuit does not overload the supply overcurrent protection or the supply wiring. Refer to the storage electrical ratings when determining the correct branch circuit rating for your installation. See Table 3 on page 12**

FIGURE 9 AC Power Connector Location



Powering On and Off

Power On the Disk System

1 Press the power button and release it. The power button will stay in a depressed position, indicating that the power is on

   See Figure 10 on page 18 for the location of the power button.

2 Confirm that the disk system is running properly by checking the system power LED and the disk module LEDs at the front of your disk system. A system reboot may be necessary to assure that the host system recognizes the disk drives within the disk system.

   Refer to "Front Panel" on page 3 for explanations of the LED functions and their meanings.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 589
3698
Doc.

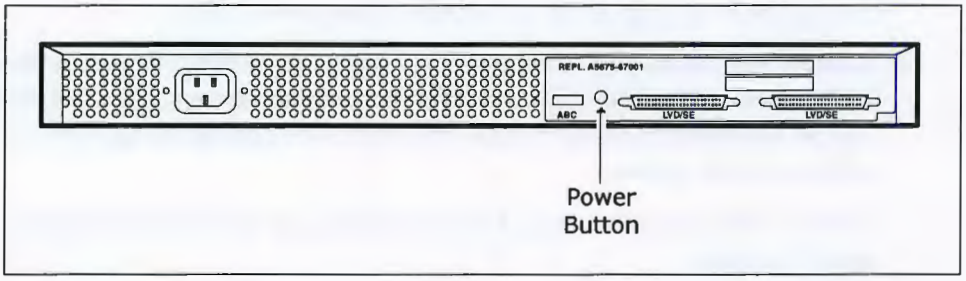
Power Off the Disk System

1. Back up all data if the disk system is still operational.
2. Ensure that no data on disk modules within the disk system is being accessed.
3. Unmount any file systems associated with the disk system that is going to be powered off. Refer to the system administration manual for your host system's operating system for the correct procedure for unmounting a file system or stopping access to the disk modules within the disk system.

> **Note** If your host system's boot or root disk drive resides in the disk system, the host system must be brought down before the power to the disk system can be turned off. See your host system's system administrator's manual for the correct procedures.

4. Turn the disk system off by pressing the power button. See Figure 10 (below) for the power button location.
5. Confirm that the storage disk system System Power LED is off. See Figure 2 on page 9
6. Disconnect the power cable from the power connector at the rear of the disk system.

FIGURE 10 Power Button Location



Adding Disk Modules

Disk modules can be added, removed, and replaced while the disk system is running. Because the disk modules can be handled in this way, they are called hot-pluggable.

The SCSI addresses for the disks are set using the addressing switches on the back of the disk system. You can determine the assigned SCSI addresses by looking at the SCSI address switch settings at the rear of the disk system.

If your storage system contains less than 4 disk modules, the remaining empty slots require filler panels. These filler panels ensure that the proper cooling is maintained within the storage system.

The system administration procedure for adding a disk modules is operating system specific. You must decide where the disk module is to be installed and install it. Then the operating system has to be configured to recognize the new disk drive.

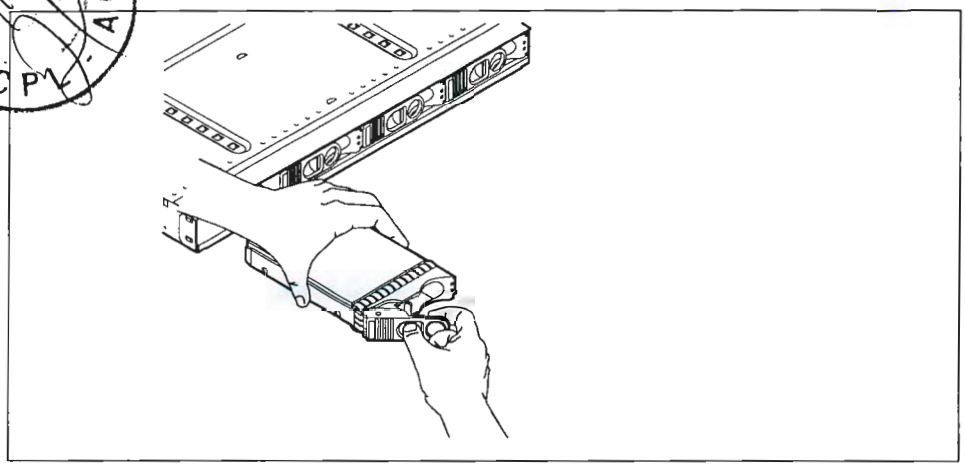
> **Note** The disk system supports the 18 and 36 GB disk capacity points. It supports these capacities in 10,000 RPM disk modules only at this time.

Add a Disk Module

1. Select an available slot for the new disk module. Note the slot chosen for application configuration.
2. Remove the disk module filler panel. Store the filler panel for future use.
3. Hold the locking handle open on the disk drive. Push the locking lever to the left to release the latch.
4. Slide the disk into the appropriate slot.
5. Gently push the drive until the locking mechanism engages. When the disk modules is completely installed, an audible click can be heard.
6. Close the locking handle completely, using gentle downward pressure.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 590
3698
Doc.

FIGURE 11 Installing a disk module



Configure the new Disk Module

Configure a New Disk Module within Your Application

CAUTION **These procedures should be performed only by qualified system administrator. Performing hot-plug operations on an active disk drive can result in data loss or corruption.**

Remove and Replace A Disk Module

Removing a Disk Module

CAUTION **If the disk system is running and a disk module slot does not contain a disk drive or filler panel, the disk system will not cool properly and may overheat. If you are not replacing the disk module immediately, a filler panel must be installed to maintain proper cooling.**
Ensure that you have a replacement disk or filler panel before removing the disk module from the disk system unless you are returning a defective disk system.

1 Ensure there is no activity on the drives.

If the Disk Drive LED for that disk module is flashing green, the disk drive is active. When the Disk Drive LED off, the disk module is either idle or completely off (see Table 1 on page 9). In this state, it is safe to remove the disk module.

2 Prepare the software environment to remove the drive.

See your operating system documentation for instructions and procedures required to remove a disk module. It may be necessary to unmount file systems associated with the disk drives installed in the disk system.

3 Unlatch the disk module handle and remove the disk module.

Squeeze the latch to unlock the disk module. Put a finger behind the latch and pull the disk module out until it disengages with the backplane. Leave it in its slot for two to three minutes to allow the disk drive to spin down before removing the disk module from the enclosure

If you are going to replace the disk module immediately, refer to "Replace a Disk Module" below.

If you are not going to replace the disk module immediately insert a filler panel into the open slot to assure the required cooling if you are not returning the disk system.

Replace a Disk Module

> **Note** The disk system supports the 18 and 36 GB disk capacity. It supports these capacities in 10,000 RPM disk modules only at this time.

1 Refer to your operating system documentation for requirements and procedures for replacing disk modules.

2 Align the replacement disk module with the disk module slot.

3 Slide the disk module into the slot until it engages with the backplane.

4 Press on the locking handle until it locks. You will hear an audible click when the locking mechanism is fully engaged.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 591
3698
Doc.

Remove the Disk System

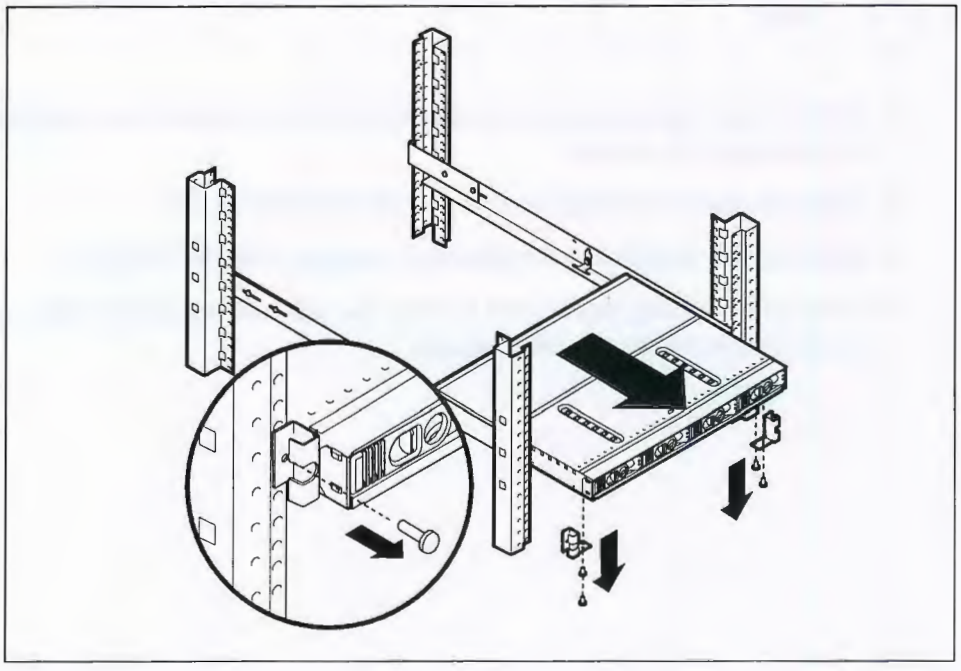
CAUTION **Some data paths may be slot-dependent. Be sure to note the slot from which the disk module is removed so it can be installed in the same slot in the replacement disk system.**

Reverse the installation instructions enclosed with the rackmount kit for your cabinet:

- A5679A for Hewlett-Packard Rack Systems/E for Enterprise Systems
- A5680A for all other Hewlett-Packard rack systems for Enterprise Systems purchased before November 1998.
- A6532A for Hewlett-Packard Rack Systems/E for Commercial Systems
- A6533A for all other Hewlett-Packard rack systems for Commerial Systems purchased before November 1998.

If your disk system is a factory-integrated unit, see the figure below for removal instructions.

FIGURE 12 Removing the Disk System



If you are returning a desktop disk system, be sure to remove and store the plastic Desktop Disk System Cover for use on the replacement disk system.

DPL

Setting Up the Hardware Event Monitor (HP-UX Only)

Hardware event monitors run on HP-UX hosts, versions 10.20 and 11.0. The Disk Monitor (disk_em) monitors all disks bound to sdisk drivers. Consequently, if the Disk Monitor is active on your host, it is already set up to monitor the disks of a new disk system. If you need to install or activate the Disk Monitor, refer to the *EMS Hardware Monitors User's Guide* in the latest IPR Support Media or on the Web (*http://www.docs.hp.com/hpux/systems/#ems*)..

> **Note** This Disk Monitor should not be confused with the EMS disk monitor that is used to monitor LVM resources.

The way you configure the monitor determines, among other things, where event messages will be sent and what level of severity will be reported.

Configuration Overview

The following steps will help you identify and resolve disk system failures:

1. Gather information from all sources:
   - Hardware event notifications (page 26)
   - Disk system LED status (page 26)
   - Online information tools (page 27)
2. Isolate the cause of the problem (Table 7 on page 31).
3. Correct the problem. (See page 20 for disk modulecremoval and replacement.)
4. Verify operational status with IOSCAN or other host utilities.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 592
3698
Doc.

Event Notification (HP-UX Only)

The Disk Monitor, an EMS hardware event monitor, reports changes in disk status. Depending on how the monitor is set up, it sends messages to the console, an e-mail address, a log file, or a third-party application. These messages give early notice of a disk problem. Events include media errors, failed read and write attempts, invalid commands, changed operating parameters, failed diagnostics, and many others.

Event severity ranges from critical to informational:

Critical	An event that causes data loss, host system downtime, or other loss of service. Host system operation will be affected if the disk system continues to be used without correction. Immediate action is required. For example, read data could not be recovered.
Serious	An event that may cause data loss, host system downtime, or other loss of service if left uncorrected. Host system and hardware operation may be adversely affected. The problem needs repair as soon as possible. For example, the request queue is full.
Warning	An event that could escalate to a serious condition if not corrected. Host system operation should not be affected and normal use of the disk system can continue. Repair is needed but at a convenient time. For example, the bus failed to reset.
Information	An event that is expected as part of the normal operation of the hardware. No action is required. For example, write protection was switched on or off.

Event messages (see Figure 13) contain the following types of information:

- Message Data – Date and time the message was sent, the source and destination of the message, and the severity level
- Event Data – Date and time of the event, the host, event ID, name of the monitor, event number, event class, severity level, hardware path, associated OS error log entry ID
- Error Description – Narrative information indicating the component that experienced the event and the nature of the event
- Probable Cause/Recommended Action – The cause of the event and suggested steps toward a solution. This information should be the first step in troubleshooting.

FIGURE 13 Sample Hardware Event Notification

```
Notification Time:  Wed Feb 3 11:27:15 1999

yourserver sent Event Monitor notification information:

/storage/events/disks/default/10_4_4_0.0 is >=1.
Its current value is CRITICAL(5)

Event data from monitor:

Event Time: Wed Feb 3 11:27:15 1999
Hostname: yourserver.rose.hp.com       IP Address : 15.43.213.13
Event ID: 0x0036b8a313000000002        Monitor    : disk_em
Event # : 100037                       Event Class: I/O
Severity : CRITICAL

Disk at hardware path 10/4/4/0.0 : Media failure
Associated OS error log entry id(s) : 000000000000000000

Description of Error:

     The device was unsuccessful in reading data for the current I/
     O request due to an error on the medium. The data could not be
     recovered. The request was likely processed in a way which
     could cause damage to or loss of data.

Probable Cause / Recommended Action:

     The medium in the device is flawed. If the medium is removable,
     replace the medium with a fresh one. Alternatively, if the
     medium is not removable, the device has experienced a hardware
     failure. Repair or replace the device, as necessary.
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 593
Doc.

Status LEDs

LEDs indicate the status of the disk system itself and each of the disk modules. A green system LED is visible on the front of the disk system. It shows that a fault has occurred or that power is on. Disk activity LEDs are on the front of the disk modules (see Figure 14 and Table 6 below).

FIGURE 14 LED Status Indicators

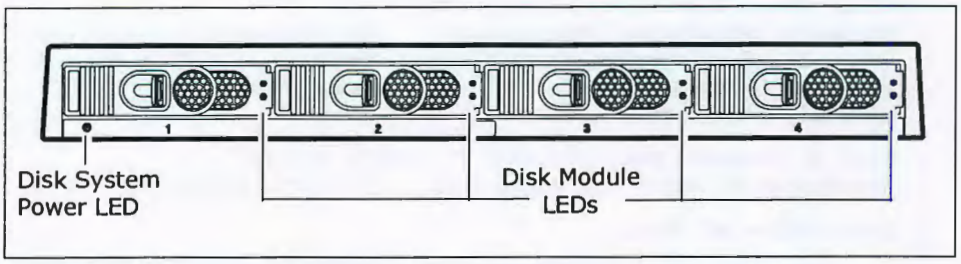


TABLE 6 LED Status Indicators

LED	State	Indication
System Power	Green	Power is on
	Blinking	Malfunction - either a fan is not operating properly or internal voltage is too low.
	OFF	Power is off
Disk Activity	ON	Installed and spinning up. If the LED is still on 3 minutes after power is engaged, the disk may be faulty.
	Flashing	I/O activity on the disk
	OFF	Not installed, not operating, or no I/O activity

English

View Disk Status

HP-UX and MPE/iX utilities provide descriptive and diagnostic information about disks, including disk type, firmware revision, and errors. On HP-UX and MPE/iX 6.5, the disk utility is Support Tools Manager (STM). For all other operating systems, consult the appropriate system administration manual for disk module status checking procedures.

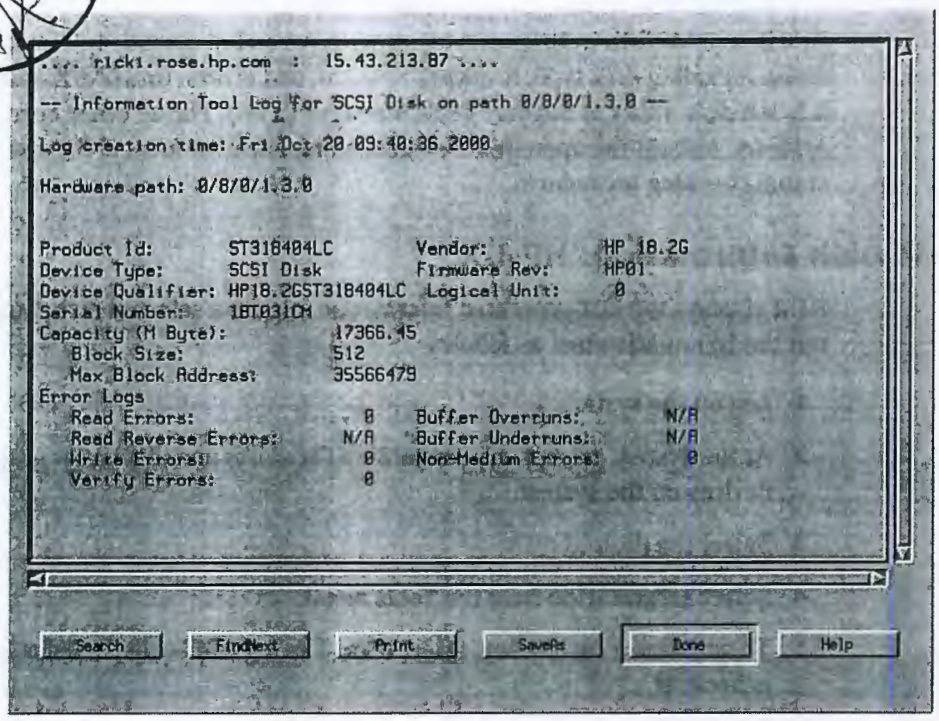
STM Disk Information: HP-UX

STM displays the last-generated Information Log for a selected disk. Start STM and run the Information tool as follows.

1. Log on the system.
2. At the system prompt, type **xstm&**. STM starts and displays a graphic of the devices on the system.
3. Select the desired disk.
4. Select **Information** from the Tools menu.
5. To generate a current log, select **Run**. The log will be displayed as soon as it is generated
6. To view a log without updating the contents, select **Information Log**.
7. Select **Done** when you have finished viewing the information.
8. To quit STM, type **exit**.
9. Figure 15 shows a sample Information Log.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 594
Doc. 3698

FIGURE 15 Sample STM Information Log (HP-UX)



E C T
C P L A C

STM Disk Information: MPE/iX 6.5 or 7.0

STM displays the last-generated Information Log for a selected disk. Start STM and run the Information tool as follows.

1. Log on the system.
2. At the system prompt (:), type **vsclose** <physical volume number>. This removes the disk from use.
3. At the system prompt (:), type **cstm**. STM starts.
4. At the cstm prompt, type **map**. STM displays a list of all the disks installed on the system.
5. Select the desired disk by typing **select device** <number>; for example, **select device 15**.
6. Type **information**. STM updates the system map.
7. To display the information log, type **infolog**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 595
Doc. 3698

FIGURE 16 Sample STM Expert Tool Disk Error Log (MPE/iX 6.5 or 7.0)

```
Write Error Statistics

     Errors Corrected Without Delay:   N/A
     Errors Corrected With Delay:      0
     Total Retries:                    0
     Total Errors Corrected:           0
     Correction Algorithm Executions:  0
     Total Bytes Processed:            6.3253e+10
     Total Uncorrected Errors:         0

Read Error Statistics

     Errors Corrected Without Delay:   23781
     Errors Corrected With Delay:      0
     Total Retries:                    0
     Total Errors Corrected:           23781
     Correction Algorithm Executions:  23781
     Total Bytes Processed:            9.6191e+10
     Total Uncorrected Errors:         0

Read Reverse Error Statistics

     Errors Corrected Without Delay:   N/A
     Errors Corrected With Delay:      N/A
     Total Retries:                    N/A
     Total Errors Corrected:           N/A
     Correction Algorithm Executions:  N/A
     Total Bytes Processed:            N/A
     Total Uncorrected Errors:         N/A

Verify Error Statistics

     Errors Corrected Without Delay:   0
     Errors Corrected With Delay:      0
     Total Retries:                    0
     Total Errors Corrected:           0
     Correction Algorithm Executions:  0
     Total Bytes Processed:            36864
     Total Uncorrected Errors:         0

Non-Medium Error Counts:               0
```

E 1025 CPL - AC

Isolating Faults

Table 7 lists the probable causes and solutions for problems you may detect on the disk system. When more than one problem describes your situation, investigate the first solution that applies. The table lists the most basic problems first and excludes them from subsequent problem descriptions.

Erratic LED behavior on the disk system could be observed in the following situations:

- When a server that is connected to a Disk System 2100 is powered down or loses power (and the disk system remains powered on)
- When the disk system is powered up when connected to a downed server
- When an unconnected disk system is powered up

An example of this LED behavior is the LEDs staying lit solidly. This condition is caused by the disk system being deprived of term power when the server loses power or is powered down. The disk system does not provide its own term power. It relies on the host bus adapter to which it is connected for term power.

TABLE 7 Troubleshooting Table

Problem Description	LED State	Probable Cause/Solution
Disk system fails to power on when installed	System power LED is off	Power cord is not plugged in. The power button is not pressed. AC breaker is tripped or AC power source has failed. The PDU/PDRU is defective. Replace. Enclosure chassis is faulty. Replace.
	System power LED is blinking	Power supply is defective - replace the enclosure Cooling fans are not spinning at the correct speed - replace the enclosure.
Operating system reports errors on a device	Disk module LED is on solid or off	Use diagnostic utilities to determine disk status. Depending on the results, monitor or replace disk module.
IOSCAN (HP-UX) lists disk as NO_HW, or Mapper or DSTAT ALL (MPE/iX) lists no device type	Disk module LED is on solid or off	Disk module is faulty - Replace. Enclosure is faulty - Replace. If the all disks on the bus have this problem, the cable is faulty. Replace the cable.
Unable to configure device for use by operating system	Disk module LED is on solid or off	Disk module possibly not correctly seated. If at a new installation, remove and reinstall the disk module. If troubleshooting an existing installation, run diagnostics to determine drive status. Replace the disk module.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 596
3698
Doc.

Reference Information

Product Numbers and Options

Three models of the disk system are available:

- A5675A field-racked disk system (Enterprise Customer Installable)
- A5675AD desktop disk system (Enterprise Systems)
- A5675AZ factory racked disk system (Enterprise Systems)
- A5676A field-racked disk system (Commerial Customer Installable)
- A5676AD desktop disk system (Commerial Systems)

TABLE 8 Products and Options

Disk System Product Number	Disk Module Product (with Option)	Description
A5675A		Field installed disk system (Enterprise)
	A6537A (0D1)	Drive integrated into the field installed disk system
	A6538A (0D1)	Drive integrated in the same field installed disk system
A5675AD		Desktop disk system (Enterprise)
	A6537A (0D1)	Drive integrated into the factory installed disk system
	A6538A (0D1)	Drive integrated in the same factory installed disk system
A5675AZ		Factory installed disk system (Enterprise)
	A6537A (0D1)	Drive integrated into the desktop disk system
	A6538A (0D1)	Drive integrated in the same desktop disk system
A5676A		Field installed disk system (Commercial)
	A6544A (0D1)	Drive integrated into the field installed disk system
	A6545A (0D1)	Drive integrated in the same field installed disk system
A5676AD		Desktop disk system (Commercial)
	A6544A (0D1)	Drive integrated into the factory installed disk system
	A6545A (0D1)	Drive integrated in the same factory installed disk system

English

Upgrade Disk Products Available

TABLE 9 Available Upgrade Disk Modules

Product Number	Description
A6537A	18-Gbyte 10,000 rpm LVD disk module (for Enterprise Systems)
A6538A	36-Gbyte 10,000 rpm LVD disk module (for Enterprise Systems)
A6544A	18-Gbyte 10,000 rpm LVD disk module (for Commerial Systems)
A6545A	36-Gbyte 10,000 rpm LVD disk module (for Commerial Systems)

TABLE 10 Upgrade Products for Hewlett-Packard Systems

Product Number	Description
A4999A	Single Port Ultra 2 SCSI Host Bus Adapter for Hewlett-Packard Workstations
A5149A	Single Port Ultra 2 SCSI Host Bus Adapter for HP-UX Systems
A5150A	Dual Port Ultra 2 SCSI Host Bus Adapter for HP-UX Systems
A5856A	Internal Disk Array Controller for HP-UX Systems
A5675A	HP Surestore Disk System 2100
A5679A	Rail kit for the Rittal Style Rack Systems and HP Rack Systems/E
A5680A	Rail kit for HP Rack Systems
A6198A	Disk Filler Panel
C2364A	LVD/SE SCSI Terminator (HDTS68)
C7430A	Ultra 2 SCSI Host Bus Adapter for HP Netservers
D2140A	Netraid 1si Host Bus Adapter for HP Netservers
D5025A	Ultrawide Host Bus Adapter for HP Netserver
D5955A	Netraid 3si Host Bus Adapter for HP Netservers
D9161A	Netraid 4M/64 Host Bus Adapter for HP Netservers
D9351A	Netraid 4M/128 Host Bus Adapter for HP Netservers
P3413A	Single Port Ultra 3 SCSI Host Bus Adapter for HP Netservers

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 597
Doc. 3698

TABLE 11 Replaceable Parts

Product Number	Description	Replaceable Part Numbers
A5675A	Base Disk System Assembly	A5675-67001
A6198A	Disk Filler Panel	A6198-60001
A6537A	18-Gbyte 10,000 rpm LVD disk module	A6537-69001
A6538A	36-Gbyte 10,000 rpm LVD disk module	A6538-69001
A6544A	18-Gbyte 10,000 rpm LVD disk module	A6544-69001
A6545A	36-Gbyte 10,000 rpm LVD disk module	A6545-69001
	Desktop Disk System Cover	5065-5217
	Desktop Disk System Feet	0403-0285

TABLE 12 Supported HP Cables and Terminators (for Enterprise Systems)

Order Number	Description	Part Number
C2978B	0.5-meter HDT S68 SCSI multimode cable	5183-2670
C2911C	1.0-meter HDT S68 SCSI multimode cable	5183-2671
C2979B	1.5-meter HDT S68 SCSI multimode cable	5183-2672
C2924C	2.5-meter HDT S68 SCSI multimode cable	5183-2673
C7521A	5.0-meter HDT S68 SCSI multimode cable	5183-2678
C2361B	1.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2674
C2362B	2.5-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2675
C2365B	5.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2676
C2364A	SCSI Terminator LVD/SE HDTS68	5183-2657

English

TABLE 13 Supported HP Cables and Terminators (for Commercial Systems)

Order Number	Description	Part Number
A6523A	0.5-meter HDT S68 SCSI multimode cable	5183-2670
A6524A	1.0-meter HDT S68 SCSI multimode cable	5183-2671
A6525A	1.5-meter HDT S68 SCSI multimode cable	5183-2672
A6526A	2.5-meter HDT S68 SCSI multimode cable	5183-2673
A6527A	5.0-meter HDT S68 SCSI multimode cable	5183-2678
A6528A	1.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2674
A6529A	2.5-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2675
A6530A	5.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2676
A6531A	SCSI Terminator LVD/SE HDTS68	5183-2657

Specifications

TABLE 14 Physical Dimensions

Measure	Metric	English
Width	45.08 cm	17.75 in
Depth	38.10 cm	15.0 in
Height	4.32 cm	1.7 in
Weight without disk modules	4.94 kg	10.90 lbs
Weight fully loaded	8.11 kg	17.89 lbs

Electrical Specifications

TABLE 15 AC Power Requirements

Electrical Element	Requirement
AC Operating Voltage Range	88-269 VACRMs
Line Frequency Range	47-63 Hz
Published Product Operating Range	100 - 240 VACRMs
Published Product Frequency Range	50 - 60 HZ

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 598
Doc. 3698

TABLE 16 Environmental Specifications

Climate Control		
Temperature (dry bulb)	Operating	0°C - +40°C
	Storage	-40°C - +70°C
Relative Humidity (non-condensing)	Operating	5% - 95% Relative Humidity at 40°C
	Storage	90% Relative Humidity at 65°C
Altitude (based on disks)	Operating	-1000 ft to +10,000 ft (3048 M)
	Storage	40,000 ft (12,092 M)
Heat Dissipation (maximum)	Operating	< 100 watts

Operating Temperatures

If the storage system is installed in a multi-unit rack assembly, the operating ambient temperature of the rack environment may exceed room ambient temperature. The rack environment ambient temperature cannot exceed 40° Celsius (104° Fahrenheit).

If your storage system contains less than 4 disk modules, the remaining empty slots require filler panels. These filler panels (part number A6198-60001) ensure that the proper cooling is maintained within the storage system.

Regulatory Statements

Safety Certifications

UL listed, UL 1950:1995 – 3rd Edition

CSA certified, C22.2 No. 950:1989

TUV certified with GS mark, EN 60950:1992 + A1:1993, A2:1993, A3:1995, A4:1997

CE mark (see on page 39)

EMC Compliance

Australia: AS/NZS 3548, Class B

Canada: ICES-003, Class B

China: GB9254-88

European Union: EN55022 Class B, EN55024

ANATEL

Japan: VCCI Class B

Taiwan: CNS 13438, Class A

US: 47 CFR Parts 2 & 15, Class B

A. FCC Notice for United States

The Federal Communications Commission (in 47 CFR 15.105) has specified that the following notice be brought to the attention of the users of this product.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antennna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Hewlett-Packard's cerification tests were conducted with a Hewlett-Packard supported computer system and Hewlett-Packard shielded cables, such as those you received with your storage product. Changes of modificaitons not expressly approved by Hewlett_packard could void the user's authority to operate the equipment. cables used with this device must be properly sheilded to comply with the requirements of the FCC.

B. FCC Notice for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
3698
Doc.

C. Notice for Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。
取り扱い説明書に従って正しい取り扱いをして下さい。

Harmonics Conformance (Japan)

高調波ガイドライン適合品

D. Notice for Taiwan

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

E. Notice for Korea

사용자 안내문 (B급 기기)

이 기기는 비업무용으로 전자파장해검정을 받은기기로서, 주거지역에서는 물론 모든 지역에서 사용 할 수 있읍니다.

F. Notice for Germany

Schalldruckpegel Lp = 55.0 dB(A)

Am Arbeitsplatz (operator position)

Normaler Betrieb (normal operation)

Nach ISO 7779:1999 (Typprüfung)

English

DECLARATION OF CONFORMITY
according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747
USA

declares, that the product

Product Name: HP SureStore Disk System 2100

Model Number(s): A5675A, A5675AD, A5675AZ, A5676A, A5676AD

Product Options: All

conforms to the following Product Specifications:

Safety: IEC 950:1991 + A1, A2, A3, A4 / EN 60950:1992 + A1, A2, A3, A4, A11
GB 4943-1995

EMC: CISPR 22:1997 / EN 55022:1998 Class A[1]
GB 9254-1988
CISPR 24:1997 / EN 55024:1998
IEC 61000-3-2:1995 / EN 61000-3-2:1995
IEC 61000-3-3:1994 / EN 61000-3-3:1995
FCC Title 47 CFR, Part 15[2]

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The product was tested in a typical configuration with a Hewlett-Packard computer system and peripherals.
2) The product complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
   - this device may not cause harmful interference; and
   - this device must accept any interference received, including interference that may cause undesired operation.

Roseville, December 6 , 2000

Frank L. Sindelar, NSSO Regulatory Mgr.

North American Contact: Hewlett-Packard Company Product Regulations Manager, 3000 Hanover Street, Palo Alto, CA 94304 Phone: 650-857-1501

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 130, D-71034 Böblingen (FAX: + 49-7031-14-3143)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 610
3698
Doc.

Product Web Site

This guide is available in Adobe® Acrobat® format on the HP Customer Care web site for enterprise storage (*http://www.hp.com/essd/*). The complete URL is *www.hp.com/support/ds2100*

Related Documents

The following manuals explain how to use the system software interfaces to the HP Surestore Disk System 2100:

- *Online Diagnostics (for HP 9000): Support Tools Manager Overview*, available at *http://www.docs.hp.com/hpux/systems/*
- *HP-UX System Administration Tasks Manual*, HP Order No. B2355-90079
- Window's NT installation guide for HP Netservers: (NT 4.0) *http://netserver.hp.com/netserver/docs/download.asp?file=it_nt_5_5_00.pdf*
- Window's NT installation guide for HP Netservers: (NT 2000) *http://netserver.hp.com/netserver/docs/download.asp?file=it_win2k_5_1_00.pdf*
- Window's NT installation guide for Legacy HP Netservers: (NT 4.0) *http://netserver.hp.com/netserver/docs/download.asp?file=ig_mwnt40.pdf*

Reader Comment Sheet

Hewlett-Packard SureStore Disk System 2100 User Guide

We welcome your evaluation of this manual. Your comments and suggestions will help us improve our publications. Remove this page and mail or FAX it to 916-785-2299. Use and attach additional pages if necessary.

	Agree				Disagree	N/A
The manual is well organized.	○	○	○	○	○	○
The information is technically accurate.	○	○	○	○	○	○
Information is easy to find.	○	○	○	○	○	○
Step-by-step procedures are easy to perform.	○	○	○	○	○	○
There are enough examples and pictures.	○	○	○	○	○	○
The examples and pictures are useful.	○	○	○	○	○	○

Comments _____

_____

_____

_____

Name: _____ Phone: _____

Title: _____ FAX: _____

Company: _____ E-mail: _____

Address: _____ ZIP: _____

City & State: _____ Country: _____

___ Check here if you would like a reply.

Hewlett-Packard has the right to use submitted suggestions without obligation, with all such ideas becoming the property of Hewlett-Packard.

HPSO/MSO Roseville Information Engineering A5675-90901 E0301

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 601
Doc. 3698

C

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 256 ROSEVILLE, CA

POSTAGE WILL BE PAID BY ADDRESSEE

Attention: Information Engineering (MS5668)

Hewlett-Packard Company
HP Storage Organization/ MSO
8000 Foothills Boulevard
Roseville, CA 95747-9987

Fold Here

Please Do Not Staple

Tape

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 602
Doc. 3698

hp OpenView storage data protector 5.0 supported devices

Version 1.15 Date: July 17, 2003

This matrix displays support for both FC/SAN environments and direct SCSI-to-SCSI connections. All media technologies and devices listed as supported with HP-UX, Windows, AIX, Tru64, Linux, Netware and Solaris are supported in both a FC/SAN environment and in a direct SCSI-to-SCSI connection. Support listed for SNI Unix, SCO Unix and MPE is valid only for SCSI-to-SCSI connections. Data Protector supports only library and drive combinations supported by the hardware vendor.

The tables below list the media technology and backup devices that are certified and supported with Data Protector 5.0. If both the media technology and the device/library are listed as supported upon the operating system on which it is to be connected, Data Protector 5.0 support exists.

For example, to employ a HP Surestore 2/20 containing HP LTO Ultrium drives with Data Protector 5.0 upon HP-UX, from checking the two tables below you will see that both the device and media technology are supported. Therefore, this is a supported Data Protector 5.0 configuration.

Although other devices may work with Data Protector 5.0, Hewlett-Packard only supports those listed within this document.

Explanation of symbols used within the matrix:

✓ refers to full Hewlett-Packard support.

● refers to devices that have been qualified as interoperable in HP-UX environments and supported with Data Protector 5.0. Please refer to HP 'third party mass storage devices'.

☑ refers to 'Referenced Support'. Referenced Support incorporates full Hewlett-Packard support for Data Protector 5.0. However, for any device related issues, please contact the corresponding product vendor first:

- ATL: 1-949-477-7924 (USA) or 44-1256-818-300 (United Kingdom)
- StorageTek: 1-800-525-0369 (USA)
- ADIC: 1-303-792-9700 (USA) or 33-0-1-30-87-53-00 (Europe)
- IBM: 1-800-772-2227 (USA)
- Sony: 1-800-883-6817 (USA)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 603
Doc. 3608

In addition, be aware of the following:

- For all devices listed below, please check the hardware I/O bus configuration with your device vendor to make sure your device also supports the I/O bus architecture.

- Data Protector 5.0 supports mixed media libraries. For further information please refer to the Data Protector 5.0 Administrator's Guide (Chapter 2, page 35).

- The IBM AIX and SNI Unix media agent supports drives only; the library robotic must be connected to a system that supports an Data Protector Media Agent with robotic support i.e. an HP-UX, Sun Solaris, Linux or a Windows system.

- On HP-UX libraries with more than one SCSI interface, the robotic control is not supported on an EISA-SCSI card.

- On Novell Netware, fibre channel attached devices must not have SCSI ID (or target ID) higher than 6.

- Cartridge Memory is supported only with HP LTO Ultrium tape drives, cartridge memory is not supported with either IBM or Seagate LTO Ultrium tape drives.

- Some devices do not support SCSI auto-configuration and must be configured manually.

- Data Protector allows the sharing of multi-drive libraries (with more than one SCSI-II interface) between multiple systems and multiple cells, the robotic control running on an HP-UX, Windows NT, or Sun Solaris system.

- A library's drives and robotics can be shared between multiple cells using the Manager-of-Managers server cell and CMMDB (Centralized Media Management Database).

- The library extension license is required for supporting a library with more than 60 slots.

- Regarding NDMP, Data Protector 5.0 only supports NetApp Filer running NDMP version 2.0 local file backups.

- On Windows NT, Windows 2000 and Novell Netware the following interface cards are supported:

    - Adaptec: 2940UW, 2940U, 2940, 2944W, 2944UW, 2940U2W(LVDS), 3940, 770X family, 780X family, 29160, 39160

    - Symbios Logic SYMSY8751, SYM8951, and SYM8952; on-board SCSI chips SYM53C875 and SYM53C895

    - AMD

new	drive technology	configure with Data Protector media type	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell Netware	MPE	Tru64
	File Device	'File'	✓	✓	✓	✓	✓	✓					
	HP Rewritable MO disk	'Optical'	✓	✓6	✓								
	DDS-2	'DDS'	✓	✓		✓	✓		✓		✓		
	DDS-3	'DDS'	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	DDS-4	'DDS'	✓	✓	✓	✓	✓	✓			✓		
N	DAT72	'DDS'	✓		✓	✓	✓	✓			✓		
	DLT4000	'DLT'	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	DLT7000	'DLT'	✓	✓	✓	✓	✓		✓	✓	✓		✓12
	DLT8000	'DLT'	✓	✓	✓	✓	✓	✓			✓	✓	✓12
	DLT1	'DLT'	✓	✓	✓	✓	✓	✓					
	DLT VS80	'DLT'	✓	✓	✓	✓	✓	✓			✓		
	DLT VS160	'DLT'			✓	✓		✓					
	SuperDLT 220	'SuperDLT'	✓	✓	✓	✓	✓	✓			✓		✓12
	SuperDLT 320	'SuperDLT'	✓	✓	✓	✓	✓	✓			✓10		✓12
	AIT-1	'AIT'		✓									
	AIT-2	'AIT'		✓	✓		✓	✓			✓		✓12
	AIT-3	'AIT'			✓	✓15	✓	✓			✓		
	DTF-1	'DTF'	☑	✓	✓								
	DTF-2	'DTF'	☑	✓	✓								
	HP LTO Ultrium 215	'LTO-Ultrium'	✓	✓	✓	✓	✓	✓			✓		
	HP LTO Ultrium 230	'LTO-Ultrium'	✓	✓	✓	✓	✓	✓			✓		
	HP Ultrium 460	'LTO-Ultrium'	✓	✓	✓	✓	✓	✓			✓		✓

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 604
Doc. 3698

new	drive technology	configure with Data Protector media type	HP-UX	Windows NT	Windows 2000/XP/2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell Netware	MPE	Tru64
	IBM Ultrium 3580 Ultrium 1[13]	'LTO-Ultrium'	☑[5]	✓	✓	✓	✓				✓		
	IBM Ultrium 2[13]	'LTO-Ultrium'			✓[14]	✓[14]	✓	✓[14]			✓[14]		✓
	Seagate LTO Ultrium Viper 200[13]	'LTO-Ultrium'		✓	✓	✓	✓				✓		
	STK4220	'T3480'	☑										
	STK4890	'T3480'		✓									
	STK9490	'T3480'	☑	✓									
	STK3480/3490e	'T3480'	☑	✓									
	STK9840A	'T9840'	☑	✓	✓	✓	✓	✓			✓		
	STK9840B	'T9840'	●	✓	✓	✓	✓	✓					
	STK9940A	'T9940'	☑[7]	✓	✓	✓							
	STK9940B	'T9940'	●		✓		✓	✓			✓		
	IBM 3590B	'T3590'	☑	✓			✓						
	IBM 3590E	'T3590'	☑	✓	✓	✓	✓						
N	IBM 3590H	'T3590'			✓		✓						
	Exabyte Eliant-820	'ExaByte'		✓									
	Exabyte Mammoth-1	'ExaByte'		✓							✓		
	Exabyte M2	'ExaByte'		✓	✓								
	Compaq TZ87	'DLT'		✓									
	Compaq TZ88	'DLT'		✓									
	Qualstar LT7000DL	'DLT'		✓									
	Qualstar T8000	'DLT'		✓									

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Optical 1300t standalone	1.3 GB	✓										
	Optical library 40st	2 drives 32 slots	✓										
	Optical library 80st	2 drives 64 slots	✓										
	Optical library 100st	2 drives 76 slots	✓										
	Optical library 165st	4 drives 120 slots	✓										
	Optical library 300st	6 drives 238 slots	✓										
	Optical library 20XT	1 drive 16 slots	✓										
	Optical library 20LT	2 drives 16 slots	✓										
	Optical library 40T	2 drives 32 slots	✓										
	Optical library 120T	4 drives 88 slots	✓										
	Optical library 200T	4 drives 144 slots	✓										
	Optical 2600fx standalone	2.6 GB	✓										
	Optical Jukebox 40fx	1 drive 16 slots	✓	✓6	✓								
	Optical Jukebox 40fx	2 drives 16 slots	✓	✓6	✓								
	Optical Jukebox 80fx	2 drives 32 slots	✓	✓6	✓								
	Optical Jukebox 160fx	4 drives 64 slots	✓	✓6	✓								
	Optical Jukebox 200fx	2 drives 76 slots	✓	✓6	✓								
	Optical Jukebox 330fx	4 drives 128 slots	✓	✓6	✓								
	Optical Jukebox 330fx	6 drives 128 slots	✓	✓6	✓								
	Optical Jukebox 600fx	6 drives 238 slots	✓	✓6	✓								
	Optical Jukebox 600fx	8 drives 238 slots	✓	✓6	✓								
	Optical Jukebox 600fx	10 drives 238 slots	✓	✓6	✓								
	Optical Jukebox 600fx	12 drives 238 slots	✓	✓6	✓								
	Optical 5200ex standalone	5.2 GB	✓	✓6	✓								

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 605
Doc. 3698

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Optical Jukebox 80ex	1 drive 16 slots	✓	✓6									
	Optical Jukebox 80ex	2 drives 16 slots	✓	✓6									
	Optical Jukebox 125ex	1 drive 24 slots	✓	✓6									
	Optical Jukebox 125ex	2 drives 24 slots	✓	✓6									
	Optical Jukebox 160ex	2 drives 32 slots	✓	✓6									
	Optical Jukebox 320ex	4 drives 64 slots	✓	✓6									
	Optical Jukebox 400ex	2 drives 76 slots	✓	✓6									
	Optical Jukebox 660ex	4 drives 128 slots	✓	✓6									
	Optical Jukebox 660ex	6 drives 128 slots	✓	✓6									
	Optical Jukebox 1200ex	4 drives 238 slots	✓	✓6									
	Optical Jukebox 1200ex	6 drives 238 slots	✓	✓6									
	Optical Jukebox 1200ex	10 drives 238 slots	✓	✓6									
	Optical 9100mx standalone	9.1 GB	✓	✓	✓								
	Optical jukebox 220mx	1-2 drives 24 slots	✓	✓	✓								
	Optical jukebox 300mx	1-2 drives 32 slots	✓	✓	✓								
	Optical jukebox 600mx	1-4 drives 64 slots	✓	✓	✓								
	Optical jukebox 700mx	1-2 drives 76 slots	✓	✓	✓								
	Optical jukebox 1200mx	1-6 drives 128 slots	✓	✓	✓								
	Optical jukebox 2200mx	1-10 drives 238 slots	✓	✓	✓								
	DAT/DDS-2 standalone	4 GB	✓	✓6		✓	✓		✓		✓		
	DAT/DDS-3 standalone	12 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	DAT/DDS2 autoloader	1 drive 6 slots		✓		✓	✓4		✓4		✓		
	DAT/DDS-2 autoloader (48AL)	1 drive 6 slots	✓	✓		✓	✓4		✓4		✓		
	DAT/DDS-3 autoloader	1 drive 6 slots	✓	✓	✓	✓	✓4	✓	✓4		✓		

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Surestore Tape 6000i/Eu	8 GB		✓		✓	✓		✓		✓		
	Surestore 12000e autoloader	1 drive 6 slots		✓		✓	✓[4]		✓[4]		✓		
	Surestore T4i/e	8 GB		✓									
	Surestore DAT8i/e/eU	4 GB	✓	✓		✓	✓		✓		✓		
	Surestore DAT24i/Eu	12 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Surestore DAT40e	20GB	✓	✓	✓	✓	✓	✓			✓		
	Surestore DAT40i	20GB	✓	✓	✓	✓	✓	✓			✓		
	Smart Storage DLT autoloader	20 GB		✓	✓	✓	✓[4]						
	Surestore DLT40e/i	20 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Surestore DLT70e	35 GB	✓	✓	✓	✓	✓		✓	✓	✓		✓[12]
	Surestore DLT80e/i/r	40 GB	✓	✓	✓	✓	✓	✓			✓	✓	✓[12]
	Surestore DLT 418 autoloader	1 drive 8 slots	✓	✓	✓								
	Surestore 718 DLT autoloader	1 drive 8 slots	✓	✓	✓								
	Surestore 818 DLT autoloader	1 drive 8 slots	✓	✓	✓	✓		✓					
	Surestore 1/15, 2/15 DLT library	1 - 2 drives 15 slots	✓	✓	✓	✓							
	Surestore 2/28 DLT library	2 drives 28 slots	✓	✓	✓	✓							
	Surestore 2/48, 4/48 DLT library	2 - 4 drives 48 slots	✓	✓	✓	✓		✓					
	Surestore 3/30 DLT library	1 - 3 drives 30 slots		✓	✓								
	Surestore 6/100 DLT library	1 - 6 drives 40 - 100 sl.		✓	✓								
	Surestore 10/588 DLT library	1 -10 drives 252-588sl.		✓	✓								
	DDS-2/DAT8 standalone	4 GB	✓	✓		✓	✓		✓		✓		
	Advanced DLT library	1- 6 drives 30 -100 sl.	✓			✓							
	Advanced DLT library	1-10 drives 252-588 sl.	✓			✓							
	Surestore DAT24 standalone	12 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 606
Doc. 360

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Smart Storage DDS-3 standalone	12 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Surestore DAT40 standalone	20 GB	✓	✓	✓	✓	✓	✓			✓		
	Smart Storage DDS-4 standalone	20 GB	✓	✓	✓	✓	✓	✓			✓		
	StorageWorks DAT72 standalone	72 GB	✓		✓	✓		✓			✓		
	Surestore DLT4000 standalone	20 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Smart Storage DLT4000 standalone	20 GB	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Surestore DLT7000 standalone	40 GB	✓	✓	✓	✓	✓		✓	✓	✓		✓12
	Smart Storage DLT7000 standalone	40 GB	✓	✓	✓	✓	✓		✓	✓	✓		✓12
	Surestore DLT8000 standalone	80 GB	✓	✓	✓	✓	✓	✓			✓	✓	✓12
	Smart Storage DLT8000 standalone	80 GB	✓	✓	✓	✓	✓	✓			✓	✓	✓12
	Surestore DLT1 standalone	40GB	✓	✓	✓	✓	✓	✓					
	DLT-VS80 standalone	80 GB	✓	✓	✓	✓	✓	✓			✓		
	Surestore Ultrium 215 standalone	200GB	✓	✓	✓	✓	✓	✓			✓		
	Surestore Ultrium 230 standalone	200GB	✓	✓	✓	✓	✓	✓			✓		
	StorageWorks Ultrium 460 LTO	400GB	✓	✓	✓	✓	✓	✓			✓		
	Surestore DAT24x6i/e autoloader	1 drive 6 slots	✓	✓	✓	✓	✓4	✓	✓4		✓	✓	
	Surestore DAT40x6i/e autoloader	1 drive 6 slots	✓	✓	✓	✓		✓			✓		
	Smart Storage DDS-3 autoloader	1 drive 6 slots	✓	✓	✓	✓	✓	✓	✓4		✓	✓	
	Smart Storage DDS-4 autoloader	1 drive 6 slots	✓	✓	✓	✓		✓			✓		
	Tape Array 5300	4 drives	✓	✓	✓	✓	✓	✓			✓		
	Tape Array 5500	5 drives	✓	✓	✓	✓	✓	✓			✓		
	1/8 series tape autoloaders	1 drive 8 slots	✓	✓	✓	✓		✓			✓		
	Surestore 1/9 autoloader	1 drive 9 slots	✓	✓	✓	✓		✓			✓		
	Surestore 1/20 tape library	1 drive 20 slots	✓	✓	✓	✓		✓			✓	✓	

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Surestore 2/20 tape library	2 drives 20 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 2/40 tape library	2 drives 40 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 4/40 tape library	4 drives 40 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 2/60 tape library	2 drives 60 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 4/60 tape library	4 drives 60 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 6/60 tape library	6 drives 60 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 6/80 tape library	6 drives 80 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 8/80 tape library	8 drives 80 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 6/100 tape library	6 drives 100 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 4/100 tape library	4 drives 100 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 10/100 tape library	10 drives 100 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 6/120 tape library	6 drives 120 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 6/140 tape library	6 drives 140 slots	✓	✓	✓	✓		✓			✓	✓	
	Surestore 10/180 Inc. mixed media support	6-10 drives 180 slots	✓	✓	✓	✓		✓			✓		✓12
	Surestore 20/700 Inc. mixed media support	20 drives 700 slots	✓	✓	✓	✓		✓			✓		✓12
	DLT 40/80 standalone	40-80GB	✓	✓8	✓8	✓	✓	✓			✓	✓	
	SDLT 110/220 standalone	110-220GB	✓	✓8	✓8	✓	✓	✓			✓		✓12
	SDLT 160/320 standalone	160-320GB	✓	✓8	✓8	✓	✓	✓			✓10		✓12
	StorageWorks AIT 35/70	35-70GB			✓8								
	StorageWorks AIT 50/100	50-100GB			✓8			✓					✓12
	StorageWorks AIT 100/200	100-200GB			✓8								
	DAT 12/24	12-24GB			✓8								
	DAT 20/40	20-40GB			✓8								
	20/40 GB 8 Cassette Autoloader	1 drive 8 slots			✓8								

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 603
Doc.

Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
DLT1 1280 SuperLooder	1 drive 16 slots		✓	✓[8]								
HP StorageWorks SSL1016 DLT1 tape autoloader	1 drive 16 slots	✓	✓	✓						✓		
HP StorageWorks SSL1016 SDLT320 tape outolooder	1 drive 16 slots	✓	✓	✓	✓		✓			✓		
HP StorageWorks SSL1016 LTO 460 tape autoloader	1 drive 16 slots	✓	✓[16]	✓[16]						✓		
SSL2020TL	1-2 drives 20 slots		✓[8]	✓[8]	✓		✓			✓		✓[12]
MSL5026DLX	1-22 drives 26 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		
MSL5026SL	1-2 drives 26 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		✓[12]
MSL5026S2	1-2 drives 26 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		✓[12]
MSL5052SL	1-4 drives 52 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		✓[12]
MSL5052S2	1-4 drives 52 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		✓[12]
MSL5030L1	1-2 drives 30 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		
MSL5060L1	1-4 drives 60 slots	✓	✓[8]	✓[8]	✓		✓			✓[9]		
HP StorogeWorks MSL6030 with Ultrium 460 tape drives	1-2 drives 30 slots	✓	✓	✓	✓							✓[12]
HP StorageWorks MSL6060 with Ultrium 460 tape drives	1-4 drives 60 slots	✓	✓	✓	✓							✓[12]
ESL9198SL	4-8 drives 198 slots	✓	✓[8]	✓[8]	✓		✓			✓		✓[12]
ESL9198DLX	4-8 drives 198 slots	✓	✓[8]	✓[8]	✓		✓			✓		
ESL9322S2	1-8 drives 322 slots	✓	✓[8]	✓[8]	✓		✓			✓		✓[12]
ESL9322LT	1-8 drives 322 slots	✓	✓[8]	✓[8]	✓		✓			✓		
HP StorageWorks ESL9322 with Ultrium 460 tape drives	1-8 drives 322 slots	✓	✓	✓	✓							✓[12]
ESL9595SL	2-16 drives 595 slots	✓	✓[8]	✓[8]	✓		✓			✓		✓[12]
ESL9595L1	2-16 drives 595 slots	✓	✓[8]	✓[8]	✓		✓			✓		
HP StorageWorks ESL9595 with Ulirium 460 tape drives	1-16 drives 595 slots	✓	✓	✓	✓							✓[12]
ESL9595S2	2-16 drives 595 slots	✓	✓[8]	✓[8]	✓		✓			✓		✓[12]
ESL9326DX	8-16 drives 326 slots	✓	✓[8]	✓[8]	✓		✓			✓		

new	Hewlett-Packard model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	ESL9326SL	8-16 drives 326 slots	✓	✓[8]	✓[8]	✓		✓			✓		✓[12]

new	Pre-merger Compaq model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	DLT 15/30 standalone	15-30GB		✓[3]									
	DLT 35/70 standalone	35-70GB		✓[3]						✓			
	TZ87 standalone	15 GB		✓[3]		✓							
	TZ88 standalone	20 GB		✓[3]		✓	✓		✓		✓		
	TZ89 standalone	35 GB		✓[3]									
	12/24 DDS-3 standalone			✓[3]									
	12/24 DAT 8 autoloader	1drive 8 slots		✓[3]	✓[3]								
	DLT 15/30 library	2 drives 15 slots		✓[3]									
	DLT 20/40 library	2 drives 15 slots		✓[3]									
	DLT 35/70 library	2 drives 15 slots		✓[3]									
	TZ877	1 drive 7 slots		✓[3]									
	TZ887	1 drive 7 slots		✓[3]									
	TL881 Base module	1-2 drives 10 slots		✓[3]									
	TL881 + expansion unit + data unit	1-10 drives 10-90 slots		✓[3]									
	TL891 Base module	1-2 drives 10 slots		✓[8]	✓[8]			✓					✓
	TL891 + expansion unit + data unit	1-10 drives 10-90 slots		✓[8]	✓[8]			✓					✓
	TL895[17]	2-7 drives 96 slots		✓[8]	✓[8]			✓					✓[12]

new	HP complementary products model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64

ECT
CPMI - CORREIOS
Fls Nº
Doc.

new	HP complementary products model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	QTM4500S DLT autoloader	1 drive 5 slots	✓										

new	StorageTek model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	SD3 standalone	50 GB	☑										
	STK4220 standalone	-	☑										
	STK9490 Timberline standalone	800 MB	☑	✓									
	STK9840 standalone	20 GB	☑	✓	✓	✓	✓						
	STK 280 scratch loader	-	☑										
	Lago LS/340 Datawheel	2 drives 25 slots		✓		✓							
	Silo Model 4400 with ACSLS	2 -16 drives 2000-6000 slots	☑	✓	✓	✓	✓						
	Silo Model 9310 Powderhorn with ACSLS[1]	2 -16 drives 2000 – 6000 slots	☑	✓	✓	✓	✓						
	Silo Model 9360 Wolfcreek	50GB 500 -1000 slots	☑	✓		✓	✓						
	STK9710 with SCSI	10 drives 252 - 588 slots	☑	✓	✓	✓							
	STK9710 with ACSLS[1]	10 drives 252 - 588 slots	☑	✓	✓	✓	✓						
	STK 9714 with SCSI	6 drives 100 slots	☑	✓	✓	✓							
	STK 9714 with ACSLS[1]	6 drives 100 slots	☑	✓	✓	✓	✓						
	STK 9730 with SCSI	3 drives 30 slots	☑	✓	✓	✓							
	STK 9730 with ACSLS[1]	3 drives 30 slots	☑	✓	✓	✓	✓						
	STK 9738 library	3 drives 30 slots		✓	✓								
	STK9740 with SCSI	10 drives 326–494 slots	☑	✓	✓	✓							

new	StorageTek model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	STK9740 with ACSLS[1]	10 drives 326 - 494 slots	☑	✓	✓	✓	✓						
	STK L20	1-2 drives 10-20 slots	●	✓	✓	✓		✓			✓		
	STK L40	2-4 drives 20-40 slots	●	✓	✓	✓		✓			✓		
	STK L80	1-8 drives 40-80 slots	●	✓	✓	✓		✓			✓		
	STK L180 with direct SCSI	10 drives 180 slots	☑	✓	✓	✓		✓			✓		✓12
	STK L180 with ACSLS[1]	10 drives 326 - 494 slots	☑	✓	✓	✓	✓						
	STK L700 with SCSI	20 drives 700 slots	☑	✓	✓	✓		✓			✓		✓12
	STK L700 with ACSLS[1]	20 drives 326–494 slots	☑	✓	✓	✓	✓						
	STK L700E with ACSLS[1]	12-20 dr. 1344 slots	☑	✓	✓	✓	✓						
	STK Silo Model L5500 with ACSLS[1]	2 -960 drives 2000 – 132,000 slots	☑	✓	✓	✓	✓						

new	Exabyte model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Eliant-820 standalone	7 GB		✓									
	Mammoth standalone	20 GB		✓									
	EZ-17	1 drive 7 slots		✓									
	18D	1 drive 8 slots		✓									
	210	1 drive 8 slots		✓									
	220	2 drives 20 slots		✓	✓								
	440/480	2-4 drives 40-80 slots		✓	✓								
	230D	2 drives 28 slots		✓									
	690D	6 drives 91 slots		✓									

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 609
Doc.

new	Exabyte model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	X80	2-8 drives 40-80 slots		✓									
	X200	2-10 drives 40-200 sl.		✓									
	215M	1-2 drives 15 slots		✓	✓								

new	Quantum model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	DLT4000 standalone	20 GB		✓	✓	✓	✓				✓		
	DLT7000 standalone	35 GB		✓	✓	✓	✓				✓		
	DLT8000 standalone	40 GB		✓	✓	✓	✓				✓		
	DLT VS160 standalone	160 GB			✓	✓		✓					
	SuperDLT 220 standalone	110GB	✓	✓	✓	✓	✓	✓			✓		
	SuperDLT 320 standalone	160GB	✓	✓	✓	✓		✓					
	DLT4500 autoloader	1 drive 5 slots		✓									
	DLT4700 autoloader	1 drive 7 slots		✓									
	520 series 2/28	2 drives 28 slots	☑	✓		✓			✓[5]				
	520 series 2/52	2 drives 28 slots	☑	✓		✓			✓[5]				
	520 series 4/52	4 drives 52 slots	☑	✓		✓			✓[5]				
	2640 series 9/88	9 drives 88 slots				✓							
	2640 series 6/176	6 drives 176 slots				✓							
	2640 series 3/264	3 drives 264 slots				✓							
	ATL PowerStor L200	1 drive 8 slots				✓							
	ATL PowerStor L500	3 drives 28 slots				✓							
	ATL P1000	2-4 drives 30 slots		✓	✓	✓							
	ATL P2000	1-10 drives 198 slots		✓	✓	✓							

new	Quantum model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	ATL 7100	2-7 drives 100 slots		✓	✓	✓							
	ATL P3000	16 drives 326 slots		✓	✓	✓							
	ATL P4000	1-10 drives 171-322 sl.		✓	✓	✓							
	ATL P7000	16 drives 679 slots		✓	✓	✓							
	ATL M1500	20 drives 200 slots		✓	✓								
	ATL M2500	15 drives 300 slots		✓	✓								
	Quantum SuperLoader	1 drive 8-16 slots			✓								

new	ADIC model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	1200D	1 drive 12 slots		✓									
	VLS 4mm	2 drives 15 slots		✓									
	VLS DLT300	1 drive 7 slots		✓									
	VLS DLT400	1 drive 7 slots		✓									
	FastStor 2	1 drive 8 slots		✓	✓	✓		✓			✓		
	FastStor 7	1 drive 7 slots		✓	✓								
	FastStor 22	1 drive 22 slots		✓	✓								
N	SCALAR 24[18]	1-2 drives 21-24 slots			✓								
	SCALAR 100	1-8 drives 24-96 slots	☑	✓	✓								
	SCALAR 218	2 drives 18 slots		✓		✓							
	SCALAR 228	2 drives 28 slots		✓		✓							
	SCALAR 448	4 drives 44 slots		✓		✓							
	SCALAR 458	4 drives 58 slots		✓		✓							
	SCALAR 1000 AML/S	1-48 drives 158-1182 slots	☑	✓	✓	✓							

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 611
Doc.

new	ADIC model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
N	SCALAR i2000[19]	1-96 drives 100-2232 slots			✓								
	SCALAR 10K	1-168 dr. 700-5000 slots		✓	✓								
	AML/J[2]	226 drives 200–4500 slots	☑	✓			✓						
	AML/E[2]	50 drives 360-11500 slots	☑	✓			✓						
	AML/2[2]	256 drives 6000-50000 slots	☑	✓			✓						

new	Overland Data model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	LXB4110 / LXB4210	1-2 drives 10 slots		✓									
	LXM4115 / LXM4215	1-2 drives 15 slots		✓									
	LXB7110 / LXB7210	1-2 drives 10 slots		✓									
	LXM7115 / LXM7215	1-2 drives 15 slots		✓									
	LXB8110/LXB8210	1-2 drives 10 slots		✓									
	PowerLoader Series	1-2 drives 15 slots		✓	✓								
	LoaderXpress Series	1 drive 10-19 slots		✓	✓								
	Neo Series LXN2000	1-16 drives 26-240 sl.			✓								
	Neo Series LXN4000	1-16 drives 52-240 sl.			✓								

new	IBM model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Archive Python	12GB		✓									
	DDS-2 standalone	4GB					✓						
	DDS-3 standalone	12GB					✓						

new	IBM model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Ultrium Tape Drive/TX200 standalone[13]	200GB	☑[5]	✓	✓						✓		
	Magstar 3590B11	1 drive 10 slots	☑	✓			✓						
	Magstar 3590E11	1 drive 10 slots	☑	✓		✓							
	IBM DDS/4 Autoloader	1 drive 6 slots		✓									
	3581 Ultrium Tape Autoloader	1 drive 7 slots	☑[5]	✓	✓	✓					✓		
	3583 Ultrium Tape Library	1-6 drives 18-72 slots	☑[5]	✓									
	3584 Ultrium Tape Library	1-72 drives 87-2481 sl.	☑[5]	✓	✓	✓		✓[11]			✓		
	3600 series	1-2 drives 20 slots		✓	✓								

new	Sony model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	SDT-9000 DDS-3 series	24 GB		✓									
	SDT-10000 DDS-4 series	20 GB		✓									
	SDX-400C AIT-1 series	35 GB		✓									
	SDX-500C AIT-2 series	50 GB		✓	✓		✓	✓			✓		
	SDX-700C AIT-3 series	260GB			✓	✓[15]	✓	✓			✓		
	TSL-A300C/TSL-SA300C AIT-1 autoloader	1 drive 4 slots		✓									
	Sony Petasite 150/80/8400	1-828 drs. 130-56,158 sl.	☑	✓	✓								

new	Dell model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	PowerVault 120T DDS	1 drive 8 slots		✓									

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 611
Doc.

new	Qualstar model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	TLS-4210	2 drives 12 slots		✓	✓	✓		✓			✓		
	TLS-4212	2 drives 14 slots		✓	✓	✓		✓			✓		
	TLS-4222	2 drives 24 slots		✓	✓	✓		✓			✓		
	TLS-4420	4 drives 22 slots		✓	✓	✓		✓			✓		
	TLS-4440	4 drives 42 slots		✓	✓	✓		✓			✓		
	TLS-4480	4 drives 84 slots		✓	✓	✓		✓			✓		
	TLS-4660	6 drives 63 slots		✓	✓	✓		✓			✓		
	TLS-46120	6 drives 126 slots		✓	✓	✓		✓			✓		
	TLS-412180	6 drives 180 slots		✓	✓	✓		✓			✓		
	TLS-412360	12 drives 360 slots		✓	✓	✓		✓			✓		
	TLS-6110	1 drive 10 slots		✓	✓	✓		✓			✓		
	TLS-6210	2 drives 10 slots		✓	✓	✓		✓			✓		
	TLS-6220	2 drives 20 slots		✓	✓	✓		✓			✓		
	TLS-6430	4 drives 30 slots		✓	✓	✓		✓			✓		
	TLS-6460	4 drives 60 slots		✓	✓	✓		✓			✓		
	TLS-68120	8 drives 120 slots		✓	✓	✓		✓			✓		
	TLS-68240	8 drives 240		✓	✓	✓		✓			✓		
	TLS-8110	1 drive 11 slots		✓	✓	✓		✓			✓		
	TLS-8211	1-2 drives 11 slots		✓	✓	✓		✓			✓		
	TLS-8222	1-2 drives 22 slots		✓	✓	✓		✓			✓		
	TLS-8466	1-4 drives 33 slots		✓	✓	✓		✓			✓		
	TLS-88132	1-8 drives 132 slots		✓	✓	✓		✓			✓		
	TLS-88264	1-8 drives 264 slots		✓	✓	✓		✓			✓		

new	Sun StorEdge model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	L8	1 drive 8 slots		✓	✓	✓		✓			✓		
	L9	1 drive 9 slots				✓							
	L20	1 drive 20 slots				✓							
	L180	10 drives 180 slots				✓							
	L280	1 drive 8 slots				✓							
	L700	20 drives 700 slots				✓							
	L1000	2-4 drives 30 slots				✓							
	L3500	2-7 drives 100 slots				✓							
	L11000	16 drives 326 slots				✓							
	L5500 with ACSLS[1]	2 -16 drives 2000 – 6000 slots		✓	✓	✓	✓						
	L6000 with ACSLS or Libstation[1]	2 -16 drives 2000 – 6000 slots		✓	✓	✓	✓						

new	Benchmark model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	ValuSmart Tape 80	40-80 GB		✓	✓	✓	✓	✓			✓		
	ValuSmart Tape VS160	80-160 GB			✓	✓		✓					
	ValuSmart Tape 640 Blade	1 drive 8 slots		✓	✓	✓		✓			✓		

new	Spectra Logic Model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Spectra 20k	2-8 drives 30-200 sl.			✓								
	Spectra 64k	2-32 drives 100-640 sl.			✓								

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 612
Doc.

new	Siemens Nixdorf Model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	PTX7-ML34	4 drives 52 slots		✓									

new	Seagate Model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Scorpion 24	24 GB		✓									
	Sidewinder 50	50 GB		✓									
	Viper 200 LTO (i/e) Standalone[13]	200 GB		✓	✓	✓	✓						
	Viper 2000 Autoloader	1drive 11 slots		✓	✓								

new	Breece Hill Model	capacity drive/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Q70 Saguaro	12 drives 70 slots		✓		✓							
	Q140 Saguaro	9 drives 140 slots		✓		✓							
	Q210 Saguaro	6 drives 210 slots		✓		✓							
	8PAC	1 drive 6 slots		✓									

new	Archive Model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	Python 20/40 DAT	20/40 GB		✓	✓								
	Python 12/24 DAT	12/24GB		✓	✓						✓		

new	MKE Model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	MKE DDS-4	12 GB		✓	✓								

new	NEC Model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	iStorage T-Series T40	2-4 drives 20-40 slots		✓	✓	✓		✓					
	iStorage T-Series T80	1-8 drives 40-80 slots		✓	✓	✓		✓					
	iStorage T-Series T180	10 drives 180 slots		✓	✓	✓		✓					
	iStorage T-Series T700	20 drives 700 slots		✓	✓	✓		✓					
	DL0101H	1 drive 10 slots		✓	✓								
	LL0101H	1 drive 10 slots		✓	✓								

new	Hitachi Model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
N	L1/20 Tape Library	1 drive 20 slots		✓	✓	✓		✓					
N	L2/20 Tape Library	2 drives 20 slots		✓	✓	✓		✓					
N	L2/40 Tape Library	2 drives 40 slots		✓	✓	✓		✓					
N	L4/40 Tape Library	4 drives 40 slots		✓	✓	✓		✓					
N	L2/80 Tape Library	2 drives 80 slots		✓	✓	✓		✓					
N	L4/80 Tape Library	4 drives 80 slots		✓	✓	✓		✓					
N	L6/80 Tape Library	6 drives 80 slots		✓	✓	✓		✓					
N	L8/80 Tape Library	8 drives 80 slots		✓	✓	✓		✓					

new	BDT Model	capacity GB/slot	HP-UX	Windows NT	Windows 2000/XP/ 2003(32bit)	Sun Solaris	IBM AIX	Linux	SNI Sinix	Sco Unix	Novell	MPE	Tru64
	ThinStor 1/8 Autoloader	1 drive 8 slots		✓	✓	✓		✓			✓		

[1] This device requires the ACSLS software from StorageTek. The following versions of ACSLS have been tested with Data Protector:

- ACSLS 5.2
- ACSLS 5.3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 619
Doc.

- ACSLS 5.3.2
- ACSLS 5.4
- ACSLS 6.0
- ACSLS 6.01

HP support covers configuration and usage of ACSLS within Data Protector, but HP provides no support for the ACSLS software. For the MVS-controlled libraries, the following versions have been tested:

- MVS 5.2.2
- Library Station 3.1.0, 4.0, 5.0
- Library Control Facility 3.1.0
- HSC 2.1.0

To utilize ACSLS on Windows NT, StorageTek LibAttach software is also required.

2 This device requires the DAS software from ADIC. The following versions of DAS have been tested with Data Protector:

- DAS 1.30
- DAS 1.30C
- DAS 3.01 (single DAS server)
- DAS 3.10

HP support covers configuration and usage of DAS within Data Protector, but HP provides no support for the DAS software.

3 For the support of these devices on these operating systems, the following SCSI controller driver is required: cpq32fs2.sys, minimum version 3.17. See the following URL:
http://www.compaq.com/support/files/server/softpaqs/WINNT/ntscsi24.html

4 Library or autoloader supported only in stacker mode.

5 To utilize IBM LTO on HP-UX, the IBM LTO for HP-UX device driver is required. This can be obtained from the following URL:
http://www.storage.ibm.com/storagesmart/lto/support/lto_ftp.htm

Please Note: The native HP-UX driver should be used for the library robotic.

6 Magneto-Optical disk support with Windows NT does not include Data Protector Enhanced Automated Disaster Recovery.

7 The STK9940 is supported with HP-UX only in STK9840 emulation mode. Please configure your STK9940 device as an STK9840 in the Omniback II GUI.

8 For the support of these devices on these operating systems, the following SCSI controller drivers are required:

For 32bit SCSI Controller - cpq32fs2.sys, version 5.12.20.
For 64bit SCSI Controller – adpu160m.sys, version 6.1.530.201

See the following URL:
http://www.compaq.com/support/files/server/softpaqs/WINNT/ntscsi24.html

9 Data Protector 5.0 'Barcode reader support' not supported.

[10] Please expect a delay when restoring data over two media with the SuperDLT 320 on Novell Netware. This will be fixed within the next Data Protector 5.0 Media Agent patch.

[11] To utilize IBM 3584 on Linux, the IBM device drivers are required. These can be obtained from the following URL:
http://www-1.ibm.com/support/all_download_drivers.html

[12] Data Protector 'devbra' command and device auto-configuration are not supported with Tru64.

[13] LTO Ultrium Cartridge Memory is not supported with IBM or Seagate LTO Ultrium tape drives.

[14] Please include Data Protector global variable OB2SHORTSEEK=500 in omnirc/.omnirc file.

[15] To utilize the AIT-3 device, the latest Data Protector Media Agent patch is required:
http://support.openview.hp.com/cpe/patches/dp/dp.jsp

[16] Insight Storage Agent should be disabled when using the HP StorageWorks SSL1016 tape autoloader with LTO 460 on Windows NT and Windows 2000/XP with the Adaptec U160 SCSI HBA.

[17] TL895 option 'Auto Drive Unload' needs to be turned to enabled (this is not the default setting).

[18] To utilize the ADIC SCALAR 24, please use the ADIC Scalar 100' sign on string.

[19] To utilize the ADIC SCALAR i2000, please use the 'ADIC Scalar 1000' sign on string.

Please Note:

If required, information regarding the Data Protector omnirc/.omnirc file can be found within the Data Protector 5.0 *Administrator's Guide*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 611
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 615
Nº 3698
Doc.

E C T
CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 616
3698
Doc.

Cooling Requirements

The temperature and humidity specifications shown below are the maximums and standards at which server cooling parameters have been established.

Temperature and Humidity Specifications				
Parameter	**Maximum Non-Operating Range**	**Recommended Operating Range**	**Maximum Operating Range**	**Rate Of Change (per hour)**
Temperature[a]	-40° C to +65° C (-40° F to 149° F)	20° to 25° C (70° to 77° F)	5° C to 35° C (41° F to 95° F)	10° C (50° F) R[b] 20° C (68° F) N[c] 20° F (-7° C) R[b] 30° F (-1° C) N[c]
Operating Humidity	5% to 90%, non-condensing at 25° C (77° F)	40% - 50%, non-condensing at 25° C (77° F)	15% - 80%, non-condensing at 25° C (77° F)	30% RH/hour

a. At altitudes up to 3,000 meters.
b. Repetitive
c. Non-repetitive

ECT
1039
Paula
CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 61
3698
Doc.

3 System Site Preparation

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 618
3698
Doc.

Other Safety/Operation Standards

The following are some of the other environmental influences that may affect L Class servers.

Vibration

Continuous vibration can cause a slow degradation of mechanical parts and, when severe, can cause data errors in disc drives. Mechanical connections such as printed circuit assembly (PCA) connectors, cable connectors, and processor backplane wiring can also be affected by vibration.

Flammable Materials

Fundamental safeguards for computer systems should include a site well away from any sources of potential damage. The system should not be installed or operated in an environment where there is a risk of fire or explosion due to the existence of highly flammable gases, volatile liquids, or combustible dust.

Airborne Contaminants

Airborne contaminants and particles of a certain size and hardness can damage your computer system, particularly disc drives. Corrosive gases and/or solvent vapors such as those from liquid spirit duplicating equipment and wet-process photo copiers can also cause damage. Some of the most common contaminants are dust, smoke, ash, eraser debris, food crumbs, and salty air.

Electrostatic Discharge

If there is an abnormally high level of static electricity at your computer system's location (15 KV or higher), anyone can cause "sparking" upon contact with the equipment. Carpeting and/or low humidity is a major source of static electricity, especially in dry and cold climates. Static electricity can often be significantly reduced by using a humidifier.

NOTE Hewlett-Packard recommends a heat evaporating-type humidifier and strongly advises against using a cold water atomizer type humidifier

Other ways to minimize electrostatic discharge are by using specially grounded mats in front of the computer system or by treating carpeting with anti-static spray. If spray is used, apply it while the system is turned off. Sprays are very temporary and must be reapplied frequently.

CAUTION Anti-static spray is not recommended because it gets into the system intake filter and coats the circuitry.

E C
9013 Tayley
C P L - C

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 619
3698
Doc.

Electrical Interference Safety Standards

The following are some of the sources of electrical interference that may affect rp24xx servers.

Convenience Wall Outlets

Power outlets for building maintenance equipment (i.e., vacuum cleaners, floor buffers, etc.) must be wired from circuit breakers on a power panel separate from the computer system panel. The ground wires from these outlets must be connected to the normal building distribution panel; not the computer system ground.

If a separate power source and separate ground are not provided, operation of janitorial equipment can induce electrical noise and cause abnormal operation of the computer system. Your electrician can verify whether or not maintenance outlets are on separate panels.

Lightning

In some geographical areas it may by advisable to install lightning protection for both personnel and computer systems. In the United States (USA), the installation of lightning or surge arrestors on power and communication lines is described in the National Electrical Code, Article 280. All lightning arrestors must have the UL 1449 rating and should be tested to survive the suite of IEEE587 tests.

The principles of lightning protection and personnel safety are outlined in detail in the lightning protection code contained in the National Fire Protection Association (NFPA) Handbook.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 620
3698
Doc.

Temperature and Humidity Operation Standards

The following table lists the computer room temperature and humidity specifications for rp24xx servers.

Temperature and Humidity Specifications				
Parameter	**Maximum Non-Operating Range**	**Recommended Operating Range**	**Maximum Operating Range**	**Rate Of Change (per hour)**
Temperature[a]	-40° C to +65° C (-40° F to 149° F)	20° to 25° C (70° to 77° F)	5° C to 39° C (41° F to 102° F)	10° C (50° F) R[b] 20° C (68° F)N[c] 20° F (-7° C)R[b] 30° F (-1° C)N[c]
Operating Humidity	5% to 90%, non-condensing at 25° C (77° F)	40% - 50%, non-condensing at 25° C (77° F)	15% - 80%, non-condensing at 25° C (77° F)	30% RH/hour

a. At altitudes up to 3,000 meters.
b. Repetitive.
c. Non-repetitive.

NOTE Operating ranges refer to the ambient air temperature and humidity measured at the cabinet cooling air intake vents.

E C T
9047
Paula
CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 621
3698
Doc.

Altitude Operation Standards

Maximum Altitude	
Operational	3000 meters above sea level
Non-operational	4572 meters above sea level

Effects of Altitude

Altitude effects the cooling of computer systems. Less air density means less cooling. Differences in air temperature, input to exhaust, can increase significantly at higher altitudes.

C T I
9049
CPqRaiz - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
FIs. Nº 622
Doc. 3698

Local Computer Installation Codes

Special local codes exist in some locations regulating the installation of computer equipment. The customer is responsible for making sure their computer system installation is in compliance with all local laws, regulations, and codes for mechanical, building, and electrical distribution systems prior to system installation. The Hewlett-Packard Site Preparation Specialist can assist in determining your local regulations.

E C T
9951
CPL - AC

RQS nº 03/2006 - CN
CPMI - CORREIOS
Fls: Nº 623
3698
Doc.

Acoustic Safety Standards

The acoustic specifications for the rp24xx server are as follows:

Sound power level	6.4 Bels LWA
Sound pressure level at operator position	58.2 dB LPA

Reducing Acoustic Noise Levels

Ambient noise level in a computer room or office environment can be reduced by the following means:

- Dropped ceiling—Cover with a commercial grade of fire-resistant, acoustic rated, fiberglass ceiling tile.
- Sound deadening—Cover the walls with curtains or other sound deadening material.
- Removable partitions—Foam rubber models reduce noise levels the best.

- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) and antistatic mats when handling circuit boards.
- Store spare electronic modules in antistatic containers.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 624
3698
Doc.

ESD Safety Standards

Static charges (voltage levels) occur when objects are separated or rubbed together. The voltage level of a static charge is determined by the following factors:

- Types of materials
- Relative humidity
- Rate of change or separation

Effect of humidity on ESD charge levels

The following table lists charge levels based on personnel activities and humidity levels.

Activity[a]	Humidity[b] and charge levels (voltages)[c]			
	26%	32%	40%	50%
Person walking across a linoleum floor	6,150 V	5,750 V	4,625 V	3,700 V
Person walking across a carpeted floor	18,450 V	17,250 V	13,875 V	11,100 V
Person getting up from a plastic chair	24,600 V	23,000 V	18,500 V	14,800 V

a. Source: B.A. Unger, Electrostatic Discharge Failures of Semiconductor Devices (Bell Laboratories, 1981)
b. For the same relative humidity level, a high rate of airflow produces higher static charges than a low airflow rate.
c. Some data in this table has been extrapolated.

Static protection measures — computer room environments

Follow these precautions to minimize possible ESD-induced failures in the computer room:

- Maintain recommended humidity level and airflow rates in the computer room.
- Install conductive flooring (conductive adhesive must be used when laying tiles).
- Use conductive wax if waxed floors are necessary.
- Ensure that all equipment and flooring are properly grounded and are at the same ground potential.
- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) and antistatic mats when handling circuit boards.
- Store spare electronic modules in antistatic containers.

Static protection measures — office environments

Office areas generally do not offer the same degree of environmental control possible in a computer room. However, some of the same precautions should be followed:

- Maintain recommended humidity level and airflow rates in the office.

Acoustics (Germany)

Acoustic noise level per ISO 9296 (25° C):

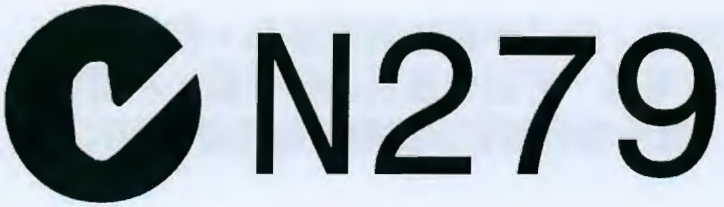
LpA_m <60dB (operators position)

Geräuschemission (Deuschland)

Geräuschemission nach ISO 9296 (25° C):

LpA_m <60dB (Arbeitsplatz)

Australian C-Tick Label



Laser Safety

This product contains a laser internal to the Optical Link Module (OLM) for connection to the Fibre communications port.

In the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. The certification is indicated by a label on the plastic OLM housing.

Outside the USA, the OLM is certified as a Class 1 laser product conforming to the requirements contained in IEC 825-1:1993 and EN 60825-1:1994, including Amendment 11:1996.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 625
3698
Doc.

Korean RFI Statement

사용자 안내문 (A급 기기)

이 기기는 업무용으로 전자파 적합 등록을 받은 기기이오니, 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Taiwan RFI Statement

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japan Safety and Regulatory Statements

高調波ガイドライン適合品

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

省エネ法による区分：K

エネルギー消費効率：0.29

エネルギー消費効率とは，省エネ法で定める測定方法により測定された消費電力を，省エネ法で定める複合理論性能で除したものである。

省エネ法による区分：G

エネルギー消費効率：0.41

エネルギー消費効率とは，省エネ法で定める測定方法により測定された消費電力を，省エネ法で定める複合理論性能で除したものである。

FCC Statement (USA Only)

The United States Federal Communications Commission has specified that the following notice be brought to the attention of users of this product:

NOTE This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Hewlett-Packard's system verification tests were conducted with HP-supported peripheral devices and HP shielded cables, such as those you receive with your computer. Changes or modifications not expressly approved by Hewlett-Packard could void the user's authority to operate the equipment. Cables used with this device must be properly shielded to comply with the requirements of the FCC.

Canada RFI Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Notice relative aux interférences radioélectriques (Canada)

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union RFI Statement

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 626
Doc.

Declaration of Conformity

DECLARATION OF CONFORMITY
according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company
Internet & Applications Systems Division

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747
USA

declares, that the product

Product Name: HP Server rp24xx (where x is any number 0-9)

Regulatory Model: RSVL-0107-A-xx (where -xx is an optional suffix and x is any letter or blank)

Product Options: All

conforms to the following Product Specifications:

Safety: IEC 60950:1991+A1+A2 +A3 +A4 /
EN 60950: 1992+A1+A2 +A3 +A4 +A11
IEC 60825-1:1993 +A1 / EN 60825-1:1994+A11, Class 1
GB 4943-1995

EMC: CISPR 22:1997 / EN 55022:1998 Class A [1)]
CISPR 24:1997 / EN 55024:1998

IEC 61000-3-2:1995 / EN 61000-3-2:1995 +A14
IEC 61000-3-3:1994 / EN 61000-3-3:1995
GB 9254-1988

Supplementary Information

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The product was tested in a typical configuration with Hewlett-Packard computer peripherals.

2) DC versions of the product were tested in a typical configuration with a Hewlett-Packard 6813A AC/DC power source.

Roseville, 11/28/01

Frank D. Dembski Jr., Quality Manager

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 130, D-71034 Böblingen (FAX: + 49-7031-14-3143)

E.T.
1659
Paula
CPL - A.C.

機箱安全措施

注意 機箱即使是空的，也很沉重，無論其中裝有設備與否，都要小心移動。
不要在粗糙不平的地面滾動機箱，也不要讓機箱傾斜超過 10 度。
無論是從運送底座上搬下機箱，還是移動機箱，都應當至少由兩個人來操作。

注意 當設備放在運送底座上時，可滑動的製品不可伸出機箱以外。讓可滑動的製品伸出機箱以前，一定要先把機箱從底座上卸下，並將前後防傾倒腳座裝好。

注意 當裝好後，前後兩個防傾倒腳座須保持這個狀態以維持穩定。一次只能讓一件可滑動的製品伸出機箱以外。

注意 要使用任何滑軌安裝產品前，須要先在機箱上安裝防傾倒裝置。
下列機箱產品的防傾倒裝置是一對防傾倒的機箱腳座：
A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, 及 J1502A

在安裝任何滑軌安裝產品前，請先安裝機箱前後的防傾倒腳座。

下列機箱產品的防傾倒裝置是安裝在機箱底部的壓艙物：
A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, 及 C2787A

要決定須要多少壓艙物，請參考機箱隨附的文件中的壓艙物工作表，
或參閱 www.docs.hp.com

不遵循這些安全措施可能會造成設備損毀或人員傷害。

RQS nº 03/2005 - CN
CPMI - CORREIOS
627
Fls Nº
Doc.

安 全 措 施

注意 空机柜也很沉重。无论机柜里是否装有设备，都要小心移动。不要在粗糙不平处滚动，也不要使机柜倾斜超过 10 度。无论是从货盘上搬下机柜，还是移动机柜，都应当由至少两个人来操作。

注意 当设备放在运输货盘上时，请勿将可滑动的产品从机柜中移出，在移动可滑动的产品之前，一定要先把机柜从货盘上卸下来，并将前后防倾倒支脚装好。

注意 装好前后防倾倒支脚后，机柜应保持稳定不动，每次只能从机柜中移出一件可滑动的产品。

注意 任何滑动安装产品均需要安装机柜防倾倒设备，下列机柜产品的防倾倒设备是一对防倾倒支脚：A4900A、A4901A、A4902A、A5134A、A5135A、A5236A、J1500A、J1501A 和 J1502A。

安装滑动安装产品之前应在机柜上安装前后防倾倒支脚。

下列机柜的防倾倒设备是在机柜底部安装的压载物：A1896A、A1897A、A1883A、A1884A、C2786A 和 C2787A。

要确定是否需要压载物，请参考随机柜一起提供文档中的压载物数据表格，或访问下面网址：www.docs.hp.com

如果不能遵守这些措施将导致设备的损坏或人员的伤亡。

CPL - AC

캐비닛 안전 주의사항

경고 캐비닛은 비어 있는 경우에도 무게가 나갑니다. 캐비닛을 운반할 때에는 안에 장비가 설치되어 있지 않더라도 항상 주의하십시오. 캐비닛을 지면에 굴곡이 있거나 수평을 이루지 않는 곳에서 회전하거나, 10 도 이상 경사로 기울이지 마십시오. 운반대서 캐비닛을 내리거나, 운반할 때에는 적어도 2 사람 이상이 수행해야 합니다.

경고 장비가 운반대에 있는 경우, 슬라이드형 제품이 캐비닛 밖으로 빠져 나오지 않도록 주의하십시오. 슬라이드형 제품을 캐비닛에서 꺼내려면, 우선 캐비닛을 운반대서 내리고 수평을 유지하기 위한 고정용 다리를 앞뒤 양쪽에 설치해야 합니다.

경고 설치를 마친 다음, 앞뒤 고정용 다리는 안정성을 위해 그대로 두십시오. 슬라이드형 제품은 한번에 두 개 이상 캐비닛에서 꺼내지 마십시오.

경고 슬라이드형 제품을 캐비닛에 넣을 경우, 수평을 유지하기 위한 장치를 사용하십시오.
다음 캐비닛 제품에 사용하는 수평 유지 장치는 두개의 고정용 다리로 되어 있습니다.
A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, J1502A

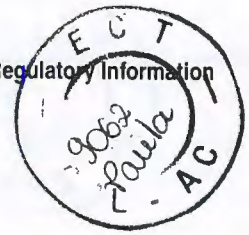
캐비닛 앞뒤 양쪽에 고정용 다리를 끼운 다음 슬라이드형 제품을 설치하십시오.

다음 캐비닛 제품에 사용하는 수평 유지 장치는 캐비닛 바닥에 까는 밸러스트입니다.
A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, C2787A

필요한 밸러스트를 보려면, 관련 캐비닛에 있는 설명서에서 밸러스트 리스트를 참조하거나, **www.docs.hp.com** 를 살펴보십시오.

수평 유지 장치를 설치하지 않은 채로 작업을 할 경우 장비가 손상되거나, 운반자가 상처를 입을 수 있습니다.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 628
3698
Doc.



キャビネットの転倒防止

注意 キャビネットは空の状態でも相当の重量があります。キャビネットに装置が搭載されていてもいなくても、移動には充分注意してください。表面に凹凸があったり水平でない場所では、キャビネットを回転したり１０度以上傾斜させることは避けてください。パレットからキャビネットを降ろしたり移動するときは最低２人以上で行ってください。

注意 装置が輸送パレットの上にある間は、スライド型製品はキャビネットの外に引き出さないでください。スライド型製品をキャビネットから引き出しておく場合は、事前にキャビネットをパレットから降ろし、傾き防止部品を前後両方とも適切に取り付けてください。

注意 設置後は、前後の傾き防止部品は安定を維持するため、取り付けたままの状態にしておいてください。スライド型製品は、一度に２台以上引き出さないでください。

警告 スライド型製品をキャビネットに組み込む場合には、あらかじめ傾き防止部品を取り付けてください。

次のキャビネットに使用する傾き防止部品は、１組のアジャスタです。
A4900A、A4901A、A4902A、A5134A、A5135A、A5136A、J1500A、J1501A、J1502A

キャビネットの前と後にアジャスタを取り付けてから、スライド型製品を組み込んでください。

次のキャビネットに使用する傾き防止部品は、キャビネットの底に取り付けるバラスト（重り）です。
A1896A、A1897A、A1883A、A1884A、C2785A、C2786A、C2787A

必要なバラストを調べるには、キャビネット付属の説明書にあるバラスト・ワークシートを参照するか、www.docs.hp.com をご覧ください。

キャビネットに傾き防止部品を取りつけないで、スライド型製品を組み込むと、装置を損傷したりけがをする恐れがあります。

Меры предосторожности при работе со стойками

ОСТОРОЖНО **Стойка очень тяжелая, даже если в ней не установлено оборудование, поэтому при ее перемещении соблюдайте меры предосторожности. Избегайте перемещения стойки по неровной поверхности или поверхности с углом наклона более 10 градусов. Снятие стойки с поддона и ее перемещение необходимо выполнять по крайней мере вдвоем.**

ОСТОРОЖНО **Оборудование, установленное на полозьях, нельзя выдвигать из стойки, пока она находится на транспортировочном поддоне. Прежде чем выдвинуть из стойки какое-либо оборудование, необходимо снять стойку с поддоиа и выдвинуть спереди и сзади стойки дополнительные опоры, предохраняющие от опрокидывания.**

ОСТОРОЖНО **Для обеспечения устойчивости стойки передние и задние опоры, предохраняющие стойку от опрокидывания, должны быть всегда выдвинуты. Никогда не выдвигайте одновременно более одного компонента оборудования, установленного на полозья.**

ОСТОРОЖНО **Перед использованием какого-либо оборудования, установленного па полозьях, необходимо устаиовить устройство, предохраняющее стойку от опрокидывания.**

Для стоек A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A и J1502A таким устройством являются две выдвижные опоры, предохраняющие от опрокидывания.

Прежде чем устанавливать на полозьях какое-либо оборудование, устаиовите спереди и сзади стойки опоры, предохраняющие от опрокидывания.

Для стоек A1896A, A1897A, A1883A, A1884A, C2785A, C2786A и C2787A в качестве устройства, предохраняющего от опрокидывания, используется балласт, который устанавливается внизу стойки.

Требования к балласту см. в документации, прилагаемой к стойке, или на Web-узле по адресу: www.docs.hp.com

Несоблюдение этих мер предосторожности может привести к травмам персонала и повреждению оборудования.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 629
Doc.

Laitekaappia koskeva turvavaroitus

WARNING **Kaapit ovat tyhjinäkin painavia. Ole varovainen siirtäessäsi kaappia siitä riippumatta, onko siihen asennettu laitteistoa. Älä rullaa kaappeja karkeilla tai epätasaisilla pinnoilla tai jos pinnan kaltevuus ylittää 10 astetta. Kaappien ottamiseen alas lastausalustalta ja niiden siirtämiseen tarvitaan ainakin kaksi henkilöä.**

WARNING **Liukuvia osia ei pidä vetää ulos kaapista laitteen ollessa lastausalustalla. Kaappi täytyy ottaa alas alustalta, ja sekä etummaisen että takimmaisen kallistustuen täytyy olla asennettu ennen liukuvien osien vetämistä ulos.**

WARNING **Kun kallistustuet on asennettu, ne täytyy jättää paikoilleen sekä edessä että takana, jotta kaappi pysyisi vakaasti paikoillaan. Vain yksi liukuosa saa olla ulkona kerrallaan.**

WARNING **Liukuviksi asennettavien tuotteiden käyttö vaatii laitekaapin kaatumisen estävän laitteen asentamista.**

Kaatumisen estävä laite laitekaapeille A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A ja J1502A on pari kaatumisen estäviä jalkoja.

Asenna sekä etu- että takajalka laitekaappiin ennen liukuviksi asennettavien tuotteiden asentamista.

Kaatumisen estävänä laitteena laitekaapeille A1896A, A1897A, A1883A, A1884A, C2785A, C2786A ja C2787A toimii painolastin asentaminen laitekaapin pohjalle.

Sopivan painolastin määrittämiseksi tutustu tuotteen mukana tulleisiin ohjeisiin (ballast worksheets) tai käy www-sivuilla osoitteessa http://www.docs.hp.com

Näiden ohjeiden noudattamatta jättäminen voi johtaa laitteiston vaurioitumiseen tai ihmisten loukkaantumiseen.

Sikkerhetsforanstaltninger for skapene

WARNING **Skapene er tunge, selv når de er tomme. Vær forsiktig når du flytter skap, uansett om de er tomme eller inneholder utstyr. Ikke rull skap på ru eller ujevne overflater eller i skråninger som heller mer enn 10 grader. Det trengs minst to personer til lessing av skap fra pallen og til flytting av skap.**

WARNING **Produkter som kan gli inn og ut av skapet bør ikke være trukket ut når skapet er på transportpallen. Skabet må lesses av pallen og anti-tippe-føtter må være påmontert både foran og bak før et produkt som kan gli inn og ut av skapet, trekkes ut.**

WARNING **Etter montering skal anti-tippe-føttene både foran og bak fortsatt være på for å opprettholde stabilitet. Produkter som kan gli inn og ut av skapet, må kun trekkes ut ett og ett om gangen.**

WARNING **Bruk av produkter som kan gli inn og ut, krever at det installeres en anti-tippe-enhet for skap.**

Anti-tippe-enheten for følgende skapprodukter er et par anti-tippe-føtter: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A og J1502A.

Installer både fremre og bakre anti-tippe-fot på skapet før du installerer produkter som kan gli inn og ut.

Anti-tippe-enheten for følgende skap er installering av ballast nederst i skapet: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A og C2787A.

Når du skal bestemme kravene til ballast, kan du se i ballastbeskrivelsen i dokumentasjonen som fulgte med skapet, eller gå til www.docs.hp.com
Hvis disse forholdsreglene ikke blir fulgt, kan det føre til skade på utstyr eller personer.

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 630
Doc. 3698

Sikkerhedsforanstaltninger for skabe

WARNING **Skabene er tunge, selv når de er tomme. Vær forsigtig når De flytter skabe, hvad enten der er installeret udstyr i skabet eller ej. Undgå at rulle skabe på ru eller ujævne overflader eller skråninger der hælder mere end 10 grader. Der skal mindst to personer til at aflæsse skabe fra pallen og til at flytte skabe.**

WARNING **Udtræksdele må ikke være trukket ud, når skabet står på forsendelsespallen. Skabet skal først læsses af pallen og anti-tip fødderne skal være installeret både forpå og bagpå, før udtræksdelene må trækkes ud.**

WARNING **Efter installation skal både de forreste og bageste anti-tip fødder blive siddende for at opretholde stabiliteten. Der må kun trækkes en udtræksdel ud ad gangen.**

WARNING **Ved enhver brug af udtræksdele skal der monteres anti-tip indretninger for skabet.**

For følgende skabstyper anvendes der som anti-tip indretning et par anti-tip fødder: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A og J1502A.

Anti-tip fødderne skal monteres både på for- og bagsiden, før der isættes udtræksdele.

For følgende skabe anvendes der som anti-tip indretning en ballast i bunden af skabet: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A og C2787A.

For beslutningen om, hvorvidt der er brug for ballast, henvises til ballasttegningerne i papirerne, der følger med skabet, samt tit www.docs.hp.com

Hvis ovenstående anvisninger ikke følges, kan det medføre materiel skade eller kvæstelse.

Voorzorgsmaatregelen voor de veiligheid voor kasten

WARNING **Kasten zijn zwaar, ook als deze leeg zijn. Ga voorzichtig te werk als u een kast verplaatst, of er nu wel of niet apparatuur in de kast is geïnstalleerd. Rol kasten niet over ruwe of ongelijke oppervlakken of hellingen van meer dan 10 graden. Als u een kast van een pallet moet afhalen of moet verplaatsen, doet u dat dan altijd met twee personen.**

WARNING **Zorg ervoor dat er geen uitschuifbare onderdelen uit de kast uitsteken als de apparatuur ter verzending op een pallet is geplaatst. Voordat u een uitschuifbaar onderdeel uitschuift, moet u de kast eerst van het pallet halen en de stabilisatiesteunen aan de voor- en achterkant op de juiste manier installeren.**

WARNING **Zodra de kast is geïnstalleerd, mogen de stabilisatiesteunen niet meer worden verplaatst. U mag niet meer dan één uitschuifbaar onderdeel tegelijk uitschuiven.**

WARNING **Als u verwisselbare opslagmedia wilt plaatsen, moet u de kast stabiliseren.**

Voor de volgende producten maakt u gebruik van stabilisatiesteunen: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A en J1502A.

U moet de stabilisatiesteunen zowel aan de voorkant als aan de achterkant van de kast aanbrengen voordat u verwisselbare opslagmedia plaatst.

De volgende kasten moet u stabiliseren door onderin de kast ballast te plaatsen: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A en C2787A.

Raadpleeg de informatie over ballast in de documentatie die u bij de kast heeft ontvangen of bezoek www.docs.hp.com om te bepalen hoeveel ballast is vereist.

Als u deze aanwijzingen niet opvolgt, kan dit leiden tot schade aan de apparatuur of lichamelijk letsel.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 631
3698
Doc.

Säkerhetsföreskrifter för kabinett

WARNING **Kabinetten är tunga även när de är tomma. Var försiktig när du flyttar ett kabinett, oavsett om det är tomt eller innehåller utrustning. Undvik att rulla kabinett på ett underlag som är ojämnt eller lutar mer än 10 grader. Det krävs minst två personer för att lasta av ett kabinett från transportpallen eller för att flytta det.**

WARNING **Inskjutningsbara produkter får inte vara utdragna när utrustningen befinner sig på transportpallen. Kabinettet måste lastas av från pallen och tippskyddsfötter ska monteras både fram- och baktill innan en inskjutningsbar produkt dras ut.**

WARNING **Efter montering ska tippskyddsfötterna sitta kvar både fram- och baktill så att stabiliteten upprätthålls. De inskjutningsbara produkterna får bara dras ut en i sänder.**

WARNING **Kabinettet måste tippskyddas för att en inskjutningsbar produkt ska kunna användas.**

För följande kabinettprodukter ska två tippskyddsfötter användas: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A och J1502A.

Installera både den främre och den bakre tippskyddsfoten på kabinettet innan du installerar en inskjutningsbar produkt.

Följande kabinett tippskyddas genom att ballast placeras i kabinettets botten: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A och C2787A.

I kabinettets dokumentation finns specifikationer för ballast. Du kan också gå till www.docs.hp.com

Om dessa föreskrifter inte följs föreligger risk för personskada eller skada på utrustningen.

Precauzioni di siccurezza sugli armadi

WARNING **Gli armadi sono molto pesanti anche quando sono vuoti. Esercitare la massima cautela durante lo spostamento degli armadi indipendentemente dal fatto che l'apparecchiatura sia installata o meno. Evitare di far scorrere gli armadi su superfici irregolari, disagevoli o con un'inclinazione superiore ai 10 gradi. Servirsi di almeno due persone sia per scaricare che per spostare gli armadi dal pallet.**

WARNING **Non aprire o estendere gli elementi scorrevoli dagli armadi mentre l'apparecchiatura è sul pallet di trasporto. Prima di estendere o aprire un qualsiasi elemento scorrevole è necessario aver scaricato gli armadi dai pallet ed aver debitamente installato gli appositi piedini antiribaltamento anteriori e posteriori.**

WARNING **Non smontare i piedini antiribaltamento dopo l'installazione perché stabilizzano gli armadi. Estendere o aprire soltanto un prodotto scorrevole per volta.**

WARNING **L'uso di qualsiasi elemento scorrevole richiede l'installazione di un dispositivo antiribaltamento.**

Il dispositivo di questo tipo adatto per i seguenti armadi è costituito da una coppia di piedini antiribaltamento: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A e J1502A.

Installare gli appositi piedini antiribaltamento anteriori e posteriori sull'armadio prima di procedere all'installazione di qualsiasi elemento scorrevole.

Il dispositivo antiribaltamento adatto per i seguenti armadi è costituito dall'installazione di un contrappeso sul fondo dell'armadio: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A e C2787A.

Per determinare i requisiti del contrappeso, fare riferimento alle schede tecniche relative comprese nella documentazione fornita con l'armadio o accedere al sito Web www.docs.hp.com

La mancata applicazione di queste norme precauzionali potrebbe causare danni all'apparecchiatura o incidenti al personale.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 692
Doc.

Procedimentos de Segurança - Armários

WARNING **Os armários são pesados, mesmo quando vazios. Tenha cuidado ao movimentar os armários, quer haja equipamentos instalados quer não. Evite deslizar os armários sobre superfícies acidentadas, irregulares ou com inclinação superior a 10 graus. A retirada dos armários do palete e sua movimentação deverão ser feitas por, no mínimo, duas pessoas.**

WARNING **Partes deslizantes não deverão ser abertas enquanto o armário encontrar-se no palete de embarque. O armário deve ser descarregado do palete e os anteparos nos pés dianteiros e traseiros devem ser instalados adequadamente antes de se abrir qualquer parte deslizante.**

WARNING **Uma vez instalados, tanto os anteparos nos pés dianteiros quanto nos traseiros devem permanecer em seus lugares adequados para garantir a estabilidade da peça. Deve-se abrir apenas uma parte deslizante por vez.**

WARNING **O uso de qualquer produto de montagem deslizante requer a instalação de um dispositivo anti-tombamento para armários.**

Um par de pés anti-tombamento é o dispositivo anti-tombamento para os seguintes armários: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, e J1502A.

Instalar ambos os pés anti-tombamento na frente e atrás do armário antes da instalação de qualquer produto de montagem deslizante.

A instalação de um lastro no fundo do armário é o dispositivo anti-tombamento para os seguintes armários: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, e C2787A.

Para determinar os requisitos de lastro, referir-se a planilha de lastro na documentação que acompanha o armário ou em www.docs.hp.com

A não observância destas precauções pode resultar em danos ao equipamento ou lesões as pessoas.

WARNING **Los productos deslizables no deben extenderse del armario cuando el equipo se encuentre en la plataforma de carga. Se debe descargar el armario de la plataforma e instalar bien las punteras delanteras y traseras de protección antes de extender cualquier producto deslizable.**

WARNING **Una vez instalado, se deberán dejar puestas las punteras de protección, delanteras y traseras, para mantener la estabilidad. Se deberá extender un solo producto deslizable cada vez.**

WARNING **El uso de cualquier producto de montaje deslizable requiere la instalación de un dispositivo de protección del armario.**

El dispositivo de protección para los siguientes armarios es un par de punteras de protección: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A y J1502A.

Instale las punteras de protección delanteras y traseras en el armario antes de instalar ningún producto de montaje deslizable.

El dispositivo de protección para los siguientes armarios es un lastre que se instala en la parte inferior del armario: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A y C2787A.

Para determinar los requisitos de lastre, consulte las hojas de datos del lastre en la documentación suministrada con el armario o bien visite www.docs.hp.com

El incumplimiento de estas medidas de precaución puede tener como resultado daños al equipo o lesiones personales.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 633
Doc. 3698

Consignes de sécurité relatives aux armoires

WARNING **Une armoire est lourde même lorsqu'elle est vide. Faites preuve de prudence lorsque vous en déplacer une, peu importe si des éléments y sont installés ou non. Évitez de faire rouler l'armoire sur un sol irrégulier ou incliné à plus de 10 degrés. Il faut au moins deux personnes pour décharger une armoire de la palette d'expédition et la déplacer.**

WARNING **Ne faites pas glisser les éléments coulissants hors de l'armoire alors qu'elle se trouve sur la palette d'expédition. Vous devez d'abord décharger l'armoire de la palette et installer correctement les pieds antibasculement, en avant et en arrière, avant de faire glisser les éléments coulissants.**

WARNING **Lorsqu'ils sont installés, les pieds antibasculement situés à l'avant et à l'arrière doivent tous deux rester en place pour assurer la stabilité de l'armoire. Vous ne devez faire glisser hors de l'armoire qu'un seul élément coulissant à la fois.**

WARNING **L'utilisation d'un élément coulissant exige l'installation préalable d'un dispositif antibasculement.**

Pour les armoires A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A et J1502A, ce dispositif consiste en une paire de pieds antibasculement.

Fixez les pieds antibasculement à l'avant et à l'arrière de l'armoire avant d'installer un élément coulissant dans cette dernière.

Pour les armoires A1896A, A1897A, A1883A, A1884A, C2785A, C2786A et C2787A, le dispositif antibasculement consiste en un contrepoids que vous devez installer au bas de l'armoire.

Pour connaître le type de contrepoids à utiliser, consultez les feuilles de travail sur les contrepoids dans la documentation qui accompagne l'armoire ou visitez le site www.docs.hp.com

Vous devez prendre ces précautions afin d'éviter des risques de dommage au matériel ou de blessure.

Medidas de seguridad para armarios

WARNING **Los armarios son pesados aun cuando estén vacíos. Tenga cuidado cuando mueva los armarios independientemente de que haya equipo instalado en el armario o no. Evite desplazar los armarios sobre superficies rugosas o disparejas o pendientes de más de 10 grados. Dos personas, como mínimo, tienen que realizar la descarga de los armarios de la plataforma de carga y mover los armarios.**

Sicherheitsvorkehrungen für Einbaugehäuse

WARNING **Einbaugehäuse haben auch ohne Inhalt ein hohes Gewicht. Seien Sie also vorsichtig, wenn Sie ein Gehäuse hin und her bewegen, sei es mit oder ohne installierten Innenteilen. Rollen Sie das Gehäuse nach Möglichkeit nicht über rauhe oder unebene Oberflächen bzw. Oberflächen mit mehr als 10 Grad Neigung. Das Abladen von der Palette und Positionieren muß von mindestens zwei Personen durchgeführt werden.**

WARNING **Ziehen Sie keine beweglichen Teile heraus, solange sich das Einbaugehäuse auf der Palette befindet. Laden Sie es zunächst von der Palette ab, und stellen Sie es mit den kippsicheren Vorder-und Hinterfüßen ordnungsgemäß auf, um bewegliche Teile sicher herausziehen zu können.**

WARNING **Nach deren Installation dürfen die kippsicheren Füße nicht wieder entfernt werden, um sicheren Stand zu gewährleisten. Ziehen Sie jeweils nur ein bewegliches Teil heraus.**

WARNING **Bevor Sie auf Gleitschienen ruhende Produkte einbauen, müssen Sie für die Kippsicherheit der Einbaugehäuse sorgen.**

Bei den folgenden Gehäuseprodukten verwenden Sie dazu in Paaren gelieferte kippsichere Füße: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A und J1502A.

Installieren Sie sowohl die vorderen als auch die hinteren kippsicheren Füße, bevor Sie auf Gleitschienen ruhende Produkte einbauen.

Bei folgenden Einbaugehäusen wird die Kippsicherheit erzielt, indem der Schrank unten mit Ballast beschwert wird: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A und C2787A.

Den erforderlichen Ballast können Sie den entsprechenden Arbeitsblättern in der Dokumentation zum Einbaugehäuse entnehmen. Außerdem finden Sie diese Informationen unter www.docs.hp.com

Eine Mißachtung dieser Sicherheitsvorkehrungen kann zu Verletzungen des Personals oder Schäden an den Geräten führen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 634
Doc. 3698

Cabinet Safety Precautions

WARNING **Cabinets are heavy even when empty. Exercise caution when moving cabinets whether equipment is installed in the cabinet or not. Avoid rolling cabinets on rough or uneven surfaces or inclines greater than 10 degrees. Unloading cabinets from the pallet and movement of cabinets should be performed by at least two people.**

WARNING **Slideable products are not to be extended from the cabinet while the equipment is on the shipping pallet. The cabinet must be unloaded from the pallet and both front and rear anti-tip feet properly installed prior to extending any slideable product.**

WARNING **Once installed, both the front and rear anti-tip feet must remain in place to maintain stability. Only one slideable product must be extended at a time.**

WARNING **Use of any slide mount product requires the installation of a cabinet anti-tip device.**

The anti-tip device for the following cabinet products is a pair of anti-tip feet: A4900A, A4901A, A4902A, A5134A, A5135A, A5136A, J1500A, J1501A, and J1502A.

Install both front and rear anti-tip feet on the cabinet before installing any slide mount product.

The anti-tip device for the following cabinets is the installation of ballast in the bottom of the cabinet: A1896A, A1897A, A1883A, A1884A, C2785A, C2786A, and C2787A.

To determine ballast requirements, refer to the ballast worksheets in documentation accompanying the cabinet or http://www.hp.com/enclosures/c_rocs.htm

Failure to follow these precautions can result in damage to equipment or injury to personnel

Regulatory Information

For your protection, this product has been tested for conformance to various national and international regulations and standards. The scope of this regulatory testing includes electrical and mechanical safety, electromagnetic emissions, immunity, acoustics and hazardous materials.

When required, approvals are obtained from third party test agencies. Approval marks appear on the product label. In addition, various regulatory bodies require some information under the headings listed in this section.

Electrical Safety

This product has not been evaluated for connection to an "IT" power system (AC distribution system having no direct connection to earth according to IEC 950).

Locate the AC outlet near the computer! The AC power cords are this product's main AC disconnect devices and must be easily accessible at all times.

Electrostatic Discharge (ESD) Precautions

When handling any electronic component or assembly (such as, a PCI card or Memory SIMM), you must observe the following antistatic precautions to prevent damage. An ESD kit (HP P/N A3024-80004) is available (or supplied with Memory additions). This kit contains one wrist strap, one conductive sheet, and one anti-static foam pad.

- Always wear a grounded wrist strap when working around the system, and when handling printed circuit boards.
- Treat all assemblies, components and interface connections as static-sensitive.
- Avoid working in carpeted areas, and keep body movement to a minimum while removing or installing boards, to minimize buildup of static charge.

Battery Notice

This product contains two Lithium batteries located on the:

- System Board
- Guardian Service Processor board

These batteries are not to be removed or replaced by the user. If either battery needs to be replaced, contact your Hewlett-Packard authorized service personnel.

CAUTION Lithium batteries may explode if mistreated.
Do not recharge, disassemble, or dispose of in a fire.

Please properly recycle all used batteries.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 635
3698
Doc.

hp Server rp24xx Safety and Regulatory Information

Overview

Regulatory Compliance statements are required by some countries for international importation of rp24xx Servers. The following information is provided:

- Regulatory Information
- Electrical Safety
  - Electrostatic Discharge (ESD) Precautions
  - Battery Notice
- Cabinet Safety Precautions
- Declaration of Conformity
- FCC Statement (USA Only)
- Canada RFI Statement
- European Union RFI Statement
- Korean RFI Statement
- Taiwan RFI Statement
- Japan Safety and Regulatory Statements
- Acoustics (Germany)
- Australian C-Tick Label
- Laser Safety

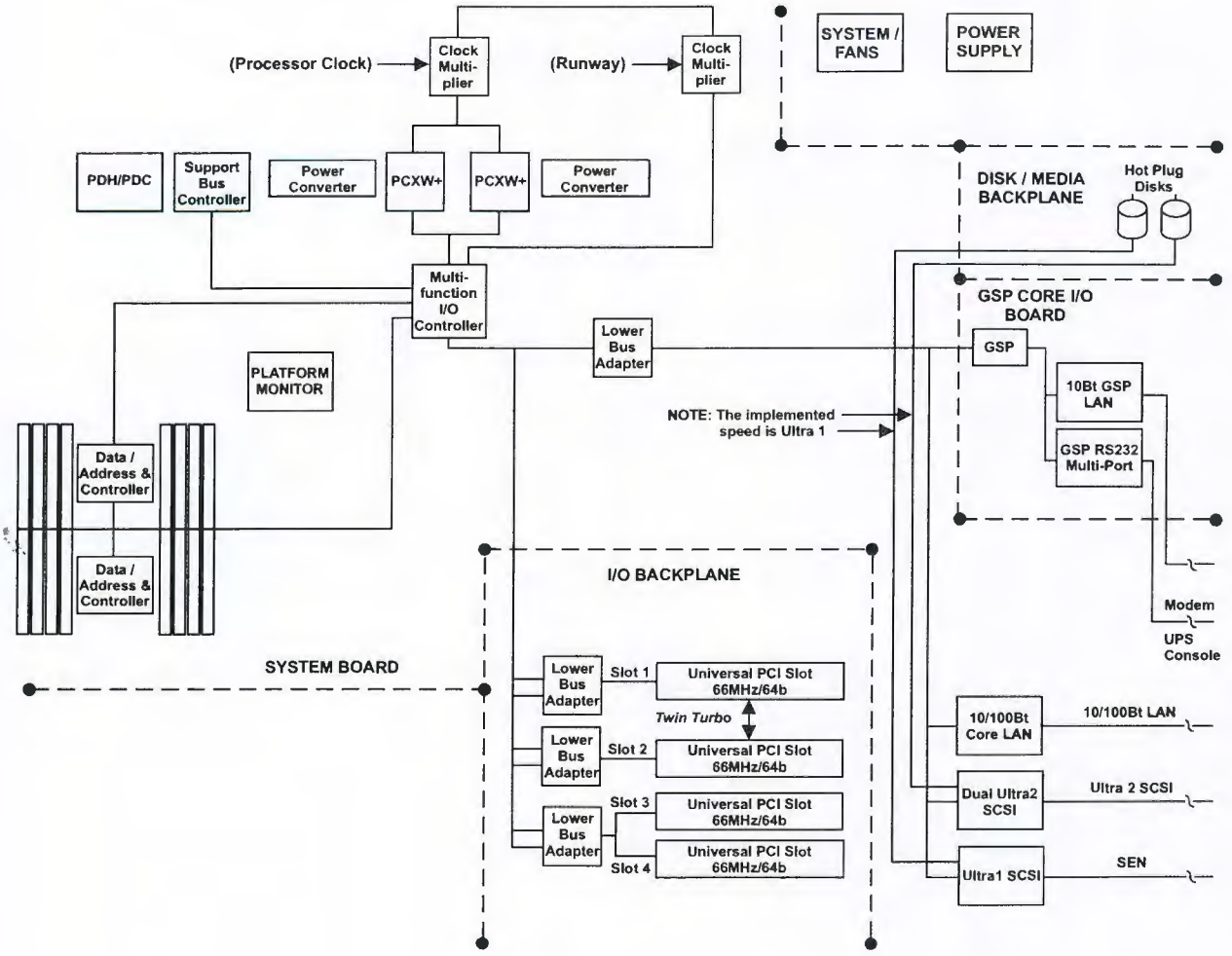
Product Information

For detailed information on the rp24xx Enterprise Server product, please go to the http://docs.hp.com web site (in the Systems Hardware selection).

E C T
1907
C. Paula
L. AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 636
3698
Doc.

rp24xx Block Diagram



ccrr016

E C T
1079
Paula
C P L - A C

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 637
3698
Doc.

System Overview

Hardware Overview

For an overview of the Enterprise Server Family hardware -

http://www.hp.com/products1/servers/family_overview.html

For an overview of the HP-9000 rp24xx Server hardware -
http://www.unixsolutions.hp.com/products/servers/aclass/index.htm

Software Requirements

rp24xx servers are designed to operate with HP-UX version 11.ACE or later.

E C T
Paula
A C

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 638
Doc. 3698

E C T
4082
Paula
A C

2 System Hardware Overview and Reference Information

ECT 9083 Paulo CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 639
Doc. 3698

What's New?

Visit this page to find out what new rp24xx server information has been released since the last web site and CD-ROM publish. The additions and modifications listed here are effective as of August 2002.

New Sections:

"What's New?" is the latest addition to the rp24xx server web site. This section will tell you about the latest changes to the previously-released information and provide a direct link to that information.

Modified Sections:

- Identified changes to all sections as applicable to HP e3000.

NOTE All references to rp24xx are equally applicable to the HP e3000.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 640
Doc. 3698

Using rp24xx Server Information

This site contains hardware support information pertaining to Hewlett-Packard rp24xx Servers. In the frame on the left side of your screen, you will see a general navigation network in a Table of Contents format. Click on the plus (or "add") sign (+) next to any topic to view the sub-topics within.

The topics were developed to support hardware-related tasks that you may need to perform in order to prepare for delivery, unpacking, installation, operation, or adding components to your rp24xx server.

There are several ways to navigate this site. The left frame will usually contain the main navigation network. The initial view in this frame is similar to a Table of Contents. However, if you wish to view a listing by topic, click on the "Index" button near the top of the screen.

Some of the topics will link to information at another site. If you are reading this information from a CD-ROM, you will need internet access to complete those links.

If you prefer to navigate this site in a more "linear" way, find the task you wish to perform, then click on that link. At the bottom of the content frame, you will see the navigation instructions to the next "logical" piece of information along with the previous "logical" piece of information.

ECT
1908
CPL AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 641
Doc. 3698

1 What's New, and Using This Information

Notice

Hewlett-Packard makes no warranty of any kind with regard to this material, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

All rights are reserved. No part of this document may be photographed, reproduced, or translated to another language without prior written consent of Hewlett-Packard Company.

The information contained in this document is subject to change without notice.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 642
3698
Doc.

rp24xx Hardware Manual

Input Power Requirements

rp24xx server input power requirements are listed as follows:

Stand Alone Server Power Requirements

- Nominal Rated Voltage: 100 or 240 VAC
- Input Voltage:

  80 to 135 VAC

  176 to 269 VAC
- Input Frequency: 47 to 66 Hz
- Input Current: 1.0 amps at maximum load with input voltage of 88 VAC and 47 Hz

If an Uninterruptible Power Supply (UPS) is to be used, ensure that it is properly connected to the server. Power cord plugs for stand-alone servers are available to meet unique power configurations used all over the world.

Cabinet Mounted Server Power Requirements

Cabinet-mounted servers have the same power requirements as stand-alone servers. However, the power cords for cabinets are dependent on the type of Power Distribution Unit (PDU).

PDU power cords with one end stripped are also available for attaching country-specific power plugs. Refer to cabinet documentation for further cabinet-specific electrical power information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 643
Doc. 3608

E C T
9034
CPL - AC

Racked Server Site Requirements

rp24xx servers can be configured to operate as a stand-alone server, in a free-standing stack of a maximum of six servers high, or racked in a cabinet. This section provides site requirements for racked server installation.

HP Cabinet Dimensions

Servers can be installed in any of the following HP cabinets:

Cabinet Product Number	Description	EIA	Max. Servers	External Dimensions (width x depth x height)	
				Centimeters	Inches
A4900A	Factory Integrated 1.25m x 19" Cabinet	25	12	59.7 x 100.3 x 125.7	23.5 x 39.5 x 49.5
A4901A	Factory Integrated 1.6m x 19" Cabinet	33	16	59.7 x 100.3 x 161.3	23.5 x 39.5 x 63.5
A4902A	Factory Integrated 2.0m x 19" Cabinet	41	20	59.7 x 100.3 x 196.9	23.5 x 39.5 x 77.5
J1502A	Field Integrated 1.25m x 19" Cabinet	25	12	59.7 x 100.3 x 125.7	23.5 x 39.5 x 49.5
J1501A	Field Integrated 1.6m x 19" Cabinet	33	16	59.7 x 100.3 x 161.3	23.5 x 39.5 x 63.5
J1500A	Field Integrated 2.0m x 19" Cabinet	41	20	59.7 x 100.3 x 196.9	23.5 x 39.5 x 77.5
C2785A	Field Integrated 1.1m x 19" Cabinet	21	10	61 x 91.4 x 111.8	24 x 36 x 44
C2786A	Field Integrated 1.6m x 19" Cabinet	32	16	61 x 91.4 x 162.6	24 x 36 x 64

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 641
3698
Doc.

Cabinet Product Number	Description	EIA	Max. Servers	External Dimensions (width x depth x height)	
				Centimeters	Inches
C2787A	Field Integrated 2.0m x 19" Cabinet	41	20	61 x 91.4 x 203.2	24 x 36 x 80

Cabinet Minimum Service Access Requirements

Access Location		
*Rear	61 cm	(24 in.)
Sides	30 cm	(12 in.)(When extended)
Front	101 cm	(40 in.)

*Minimum distance required to fully open rear access door.

Non-HP Cabinet Installation Requirements

rp24xx servers can be installed in cabinets other than those manufactured by HP. Refer to the installation instructions of the cabinet in which you wish to install the server.

WARNING **Do not install a server in any cabinet without anchoring it to the cabinet with four screws (two on each side) that attach to the front posts of the cabinet. Screws are used as a safeguard against accidental ejection in case a cabinet tips forward. rp24xx servers installed in all HP cabinets are secured with captive screws.**

HP will NOT support servers that are not secured to the cabinet with screws.

Failure to heed this warning could result in serious personal injury or damage to the server.

Stacked Server Site Requirements

rp24xx servers can be configured to operate as a stand-alone server, in a free-standing stack of a maximum of six servers high, or racked in a cabinet. This section provides site requirements for stacked server installation.

NOTE HP will not support stacking of any other A-Class server.

CAUTION In order to remain within weight limitations and to prevent tipping, do not stack servers more than six high. Each server weighs approximately 23 kg (50 lbs). DO NOT lift more than one server at a time.
Always use the strap when stacking servers, regardless of the number. Hewlett-Packard will not support or warrant servers that are damaged as a result of being improperly strapped or stacked more than six servers high.

Server Dimensions

The physical characteristics of the rp24xx server are listed as follows:

Dimension		
Height	9.52 cm	(3.75 in.)
Width	48.26 cm	(19 in.)
Depth	63.5 cm	(25 in.)
Weight	22.68 kg	(50 lbs)

WARNING **DO NOT attempt to lift the server by the front bezel. The plastic bezel is attached by pressing it onto four ball-tipped posts located on the front of the server cover and pulls off with very little pressure.**

The bezel WILL NOT support the 23 kg (50 lb.) weight of the server.

Failure to observe this precaution will cause damage to the server and may cause personal injury.

CAUTION DO NOT stack heavy objects, such as monitors, on top of the server. The weight may cause the top to cave in and damage internal components.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 645
3698
Doc.

Stacked Server Minimum Service Access Requirements

Access Location		
Rear	15 cm	(6 in.)
Sides	7.5 cm	(3 in.)
Front	7.5 cm	(3 in.)

WARNING **Ensure that the surface on which the stacked servers are sitting will support the combined weight of all servers in the stack plus the weight of all other associated equipment.**
Failure to heed this warning may result in serious injury and/or equipment damage.

E - T
9030 Paulo
CPL - AC

Stand-Alone Server Site Requirements

rp24xx servers can be configured to operate as a stand-alone server, in a free-standing stack of a maximum of six servers high, or racked in a cabinet. This section provides requirements for stand-alone server installation.

Server Dimensions

The physical characteristics of the rp24xx server are listed as follows:

Dimension		
Height	9.52 cm	(3.75 in.)
Width	48.26 cm	(19 in.)
Depth	63.5 cm	(25 in.)
Weight	22.68 kg	(50 lbs)

Stand-Alone Server Minimum Service Access Requirements

Access Location		
Rear	30 cm	(12 in.)
Left Side	15 cm	(6 in.)
Right Side	30 cm	(12 in.)
Front	30 cm	(12 in.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 646
3698
Doc.

E - T
9028 Paula
CPL - AC

Temperature and Humidity Operation Standards

The following table lists the computer room temperature and humidity specifications for rp24xx servers.

Temperature and Humidity Specifications				
Parameter	**Maximum Non-Operating Range**	**Recommended Operating Range**	**Maximum Operating Range**	**Rate Of Change (per hour)**
Temperature[a]	-40° C to +65° C (-40° F to 149° F)	20° to 25° C (70° to 77° F)	5° C to 35° C (plus or minus 2° C) (41° F to 95° F (plus or minus 3° F))	10° C (50° F) R[b] 20° C (68° F)N[c] 20° F (-7° C)R[b] 30° F (-1° C)N[c]
Operating Humidity	5% to 90%, non-condensing at 25° C (77° F)	40% - 50%, non-condensing at 25° C (77° F)	15% - 80%, non-condensing at 25° C (77° F)	30% RH/hour

a. At altitudes up to 3,000 meters.
b. Repetitive.
c. Non-repetitive.

NOTE Operating ranges refer to the ambient air temperature and humidity measured at the cabinet cooling air intake vents.

RQS nº 03/2005 - CN
CPMI - CORREIOS
647
Fls. Nº
3698
Doc.

E C T
9026
Paula
L - AC

4 Server Unpack and Install Instructions

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 648
3698
Doc.

Unpack the Server

Unpack the Server

Overview

Unpacking the server consists of opening and unloading the carton. Inside the carton you will find, in addition to the server, an accessory kit and a packet containing installation instructions and regulatory information.

NOTE The following instructions do not apply to servers that are received pre-installed in a cabinet. These procedures pertain to individual servers only.

Open and Unload the Carton

Step 1. Place the sealed carton on a work surface with the correct side up as indicated by the, "This Side Up" symbol (shown below).

WARNING **Use sharp instruments carefully when unpacking electronics equipment.**

Failure to follow this precaution may result in personal injury or damage to components.

Step 2. Carefully open the carton, remove the contents, and set them on the work surface. Each carton will contain:

- ❑ The server.
- ❑ A plastic pedestal base for holding the server in a side-mounted position
- ❑ An accessory kit.
- ❑ A packet containing installation instructions and regulatory information.

NOTE Report any missing items to your local Hewlett-Packard office immediately. If there is obvious freight damage, contact your shipper immediately.

We recommend that you retain all packing materials in case any of the items received require return to Hewlett-Packard.

Unpack the Server

WARNING **The rp24xx server weights 22.68 kg (50 lbs). Take necessary precautions to prevent muscle strain when lifting or carrying the server.**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 649
3698
Doc.

Carefully lift the server out of the carton, unwrap it, set it on the work surface.

WARNING **Do not lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency.**
Failure to heed this warning may result in personal injury and/or permanent damage to the server.

Attaching the Pedestal Base

The pedestal base and two accompanying screws included with each stand alone server provides the option of standing the server on its side in order to conserve table space, or standing the server on the floor. To install the pedestal base, follow the instructions listed below:

Step 1. As you are facing the front of the server, carefully stand it on its side with the right side up.

Step 2. Place the pedestal, smooth side down, on the server side and align it lengthwise so that it is parallel with the server.

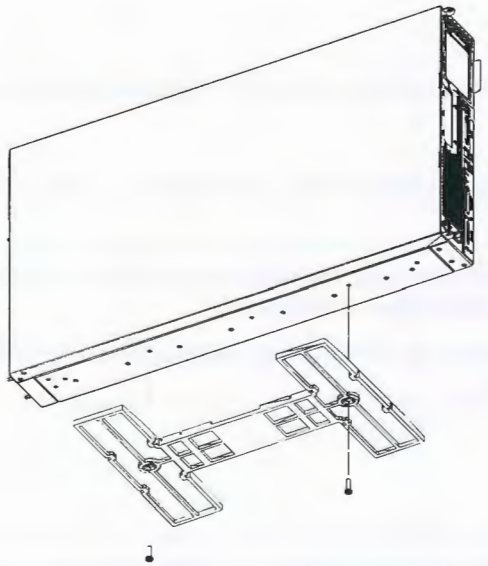
Step 3. Center the pedestal front to rear and align the two recessed oblong holes with the corresponding two holes on the server's side.

Step 4. Insert the two accompanying screws through the bottom of the pedestal and fasten securely to the server.

Step 5. Stand the server on the pedestal.

The following graphic illustrates the pedestal and server.

NOTE The bezel and cover can remain on the server when attaching the pedestal base.



Open the Accessory Kit

Open the Accessory Kit and verify that the contents agree with the packing list.

NOTE Plastic bezel end caps are included in each kit. Do not discard them. They will be needed if the server is installed in a cabinet.

A gray nylon strap is also included. Do not discard it. It will be needed to secure multiple servers (up to six) that are stacked.

Open the Installation Instructions and Regulatory Information Packet

The Installation Instructions/Regulatory Information Packet contains the following information:

- Installation Instruction Sheet, which includes:

  Basic cable connection information necessary to power on and boot the server to the Firmware Main Menu screen.

  The Universal Resource Locator (URL) for the rp24xx server page on the World Wide Web (www.docs.hp.com).

- Compact Disk (CD). Contains the same information available at www.docs.hp.com in the event that access to the Web is unavailable or inconvenient.
- Regulatory Information. Contains consumer safety and regulatory statements for the United States and for those countries that require publishing and dissemination of their own consumer safety and regulatory data.

Third Party Software

NOTE This information is not applicable to e3000 systems.

This server includes licenses for three third-party software products. Please refer to the materials contained in the shipping box for general product information and for instructions on how to download or obtain CDs with this software. The three software products are as follows:

Resonate Central Dispatch

A complimentary three-server license is included. Central Dispatch is an industry-leading enterprise traffic management software solution, ensuring up-time and performance for high traffic, mission-critical e-business applications.

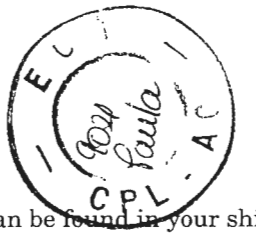
This software package can be found in your accessory box. If you cannot locate the software, or if you require an upgrade to extend the three-server license, please E-mail us at, "mailto:hpsales@Resonate.com". If you need assistance installing Central Dispatch, mail our support team at, "mailto:hpsupport@resonate.com".

You may also register for complimentary Web support for Central Dispatch. Please visit Resonate's website at "http://www.resonate.com/hp"

Infoseek Ultraseek Server

Ultraseek Server is a version of Infoseek's award-winning search technology packaged for use on your intranet or public web servers. It allows users to type question (or just keywords) and instantly find documents relating to the topic on your network.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 650
3698
Doc.



Further product information can be found in your shipping box. If you cannot locate the product information or if you need additional installation assistance, please consult the web site at http://www.ultraseek.com/hp.

Nokia Wireless Application Protocol (WAP) Server

Nokia WAP server is the industry leading WAP server software. It provides seamless functionality with most HTTP servers, retrieving native WML and WML Script content, or converting HTML content to WML.

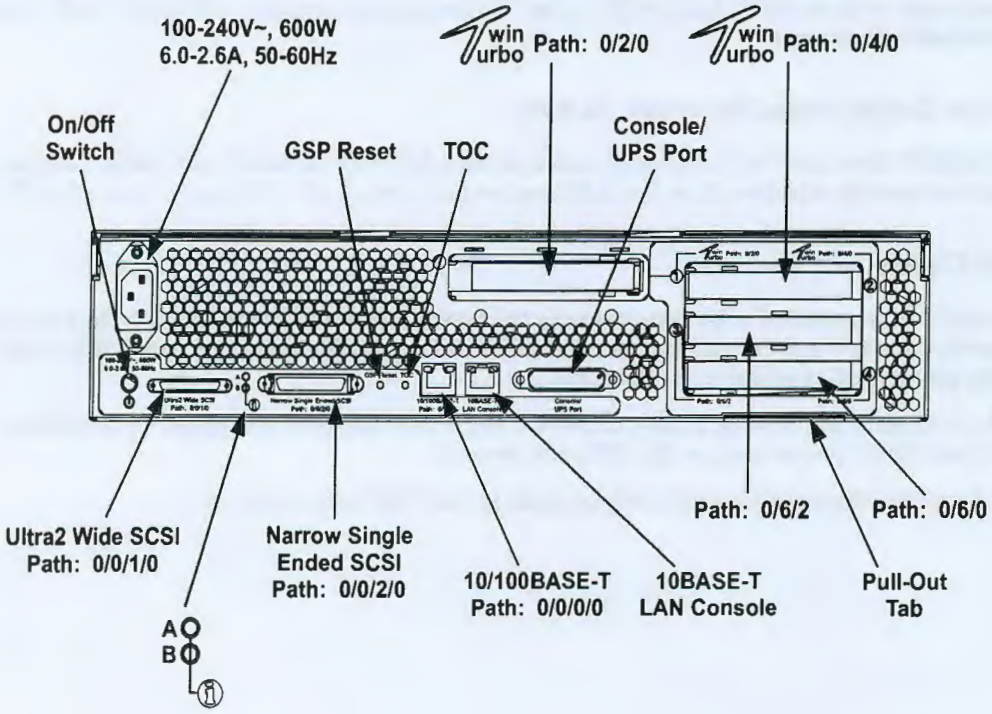
Further product information can be found in your shipping box. If you cannot locate the product information or if you need additional installation assistance, please consult our web site at "http://www.hp.com/go/mobile-aclassoffer".

Server External Connections

External devices are interfaced with the server by means of specific connectors located on the rear bulkhead. Exterior connections to the server include ports for:

- Small Computer System Interface (SCSI) devices
- System Console
- Local Area Network (LAN) Console
- LANs
- Power Cord.

The graphic shown below illustrates locations of the external connections to the server.

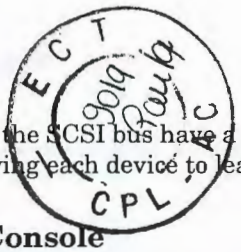


ccrr008

Connect External Small Computer System Interface (SCSI) Devices

Connect external SCSI devices to the Single Ended SCSI bus (labeled: *Narrow Single-Ended SCSI Path: 0/0/2/0)* on the system card or to the Ultra 2 SCSI bus (labeled: *Ultra 2 SCSI Path: 0/0/1/0).*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 851
3698
Doc.



Ensure that all devices on the SCSI bus have a unique address and the last device is terminated. Refer to the documentation accompanying each device to learn how to set addresses and where to place terminators.

Connect a System Console

- **Using the ASCII Terminal as a System Console**. If an ASCII terminal is to be used as a console/UPS port, make sure that the keyboard is connected and a power cable is available.
- **Using a SecureWeb Console PCI card as a System Console.** If the Secure Web Console PCI card is to be used as a system console, connect an RJ45 LAN cable to the Secure Web Console PCI card installed in an I/O card slot on the back of the server.

NOTE The Web Console has a default Internet Protocol (IP) address of 192.0.0.192. Make sure that no other device, including other rp24xx servers, has this address before connecting the server to your LAN.

- **Using the LAN Console as a System Console.** If a LAN Console is to be used as a system console, connect it to the system with an RJ45 LAN cable to the RJ45 connector labeled, *10BASE-T LAN Console* connection on the back of the server.

Connect the Core Local Area Network (LAN)

Connect the 10/100BASE-T Core LAN on the system board to the LAN with an RJ45 LAN cable. Connect the RJ45 LAN cable to the server by attaching it to the RJ45 connector labeled, *10/100 Base-T Path: 0/0/0/0*.

Connect Power Cords

Connect the power cord that is provided with the system to the server. For stand-alone servers, the power cord will be localized to each country's power application. If an HP Uninterruptible Power Supply (UPS) is the power source, use the power cord provided with the UPS.

Connect power cords to all external devices at this time with the either the localized power cord, cabinet Power Distribution Unit (PDU) power cord, or the UPS power cord.

For cabinet-mounted servers, the server power cord connects to the PDU in the cabinet.

ECT 9018 Fls CPL - A

Installing a Stand-alone Server in a Cabinet

Installing a Stand-alone Server in an HP Cabinet

The following information pertains to rp24xx server installation in cabinets manufactured by Hewlett-Packard only.

Cabinet Identification

The following HP cabinets can hold multiple HP-9000 A-Class, rp24xx servers:

Cabinet Product No.	Assembled by:	Size (Height x Width)	Max. Servers
A4900A	Factory	1.25m x 19"	12
A4901A	Factory	1.6m x 19"	16
A4902A	Factory	2.0m x 19"	20
A5134A (HPe3000)	Factory	1.25m x 19"	12
A5135A (HPe3000)	Factory	1.6m x 19"	16
A5136A (HPe3000)	Factory	2.0m x 19"	20
J1502A	Field	1.25m x 19"	12
J1501A	Field	1.6m x 19"	16
J1500A	Field	2.0m x 19"	20
C2785A	Field	1.1m x 19"	10
C2786A	Field	1.6m x 19"	16
C2787A	Field	2.0m x 19"	20

Cabinet Loading Requirements

Servers require two EIA of cabinet space (each two EIA of space is equivalent to the height of a server). Ensure that the cabinet has this amount of space available.

Fill empty cabinets from the top down. If you are mounting one or more servers into an empty cabinet, start at the inside top of the cabinet and count down four of the holes in the columns at each corner to determine the position of the rails for the first server. When the first rails are installed, continue to use the four hole requirement as your guide for installing additional rp24xx servers.

Installing the Server

The following procedure describes how to install a stand-alone server into an approved cabinet on a slide-rail assembly.

Step 1. Ensure that the anti-tip stabilizers or cabinet ballast are properly installed on the cabinet and secured.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 652
Doc.

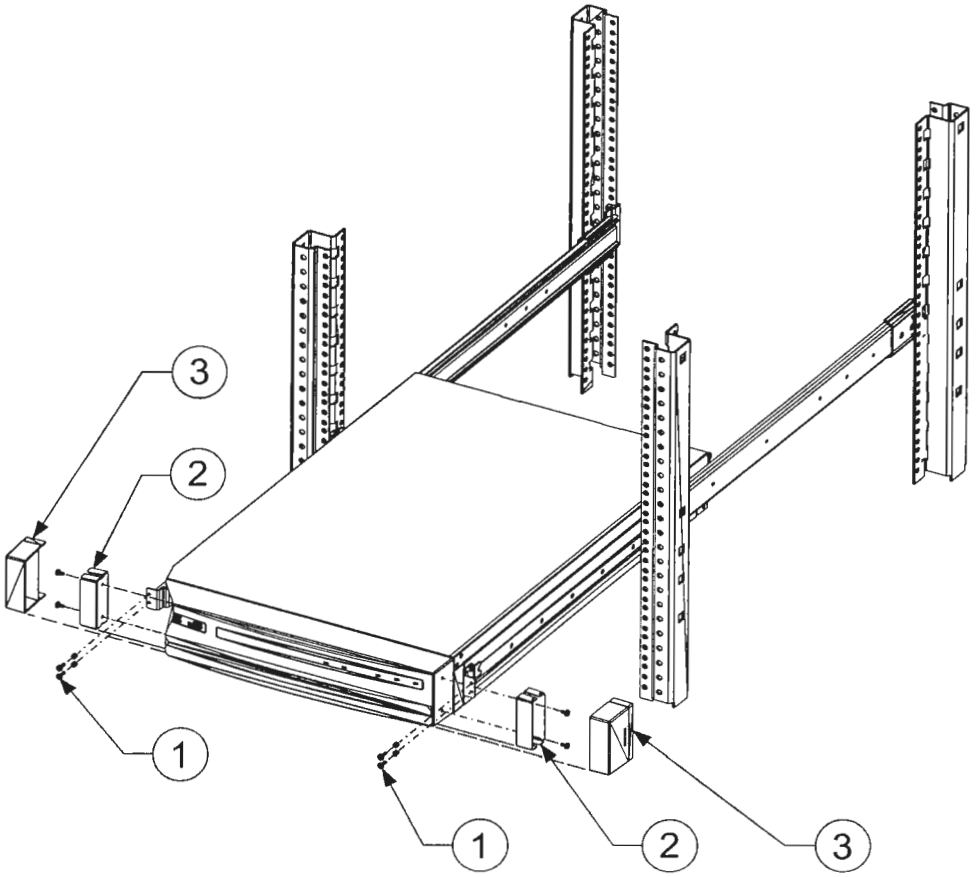
WARNING **If anti-tip stabilizers or ballast are not installed or are improperly installed on the cabinet, it can tip. Failure to follow this precaution can cause personal injury or death and can damage equipment.**

Step 2. Remove the stand alone server from it's packing materials, if not already unpacked.

Step 3. Refer to the *A-400/A-500 Server Slide Rail Installation* instructions, for both server and cabinet rail installation instructions.

Installing Bezel End Caps

Each server is shipped with two metal brackets and two plastic end caps that are designed to be attached to a stand alone server if it is to be mounted in a cabinet. Locate these items and have them available for installation. The following diagram shows the location of bezel end caps and brackets on a racked server.



ccrr001

Callout #	Item
1	Server-to-cabinet attachment screws

Callout #	Item
2	Metal brackets
3	Plastic end caps

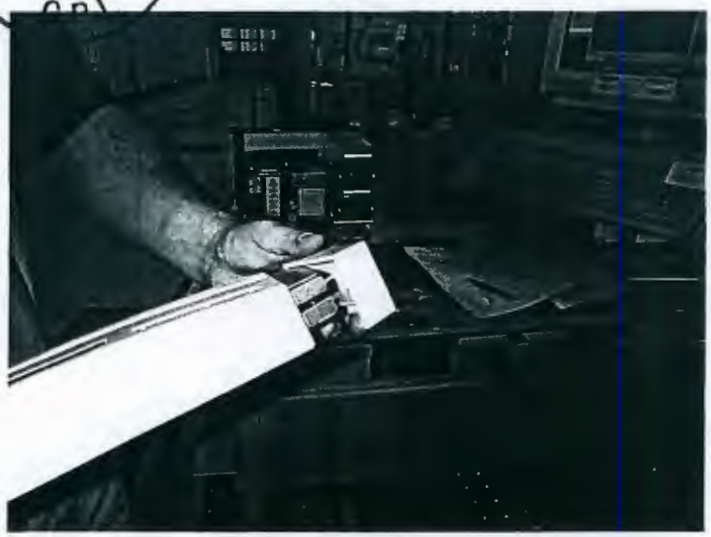
Once the rail kit has been installed and the server is positioned in the cabinet, follow the procedure listed below to attach the brackets and end caps:

Step 1. Extend the server between four and six inches out of the cabinet to allow room to work.

Step 2. Attach the metal brackets to each end of the bezel with two plastic retainers, as shown in the following graphic.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls_Nº 653
3698
Doc.

Step 3. Fit the plastic end caps over the metal brackets as shown below.



Step 4. Push the server back into the cabinet until it is flush against the vertical columns. Replace the screws that fasten the server to the rack.

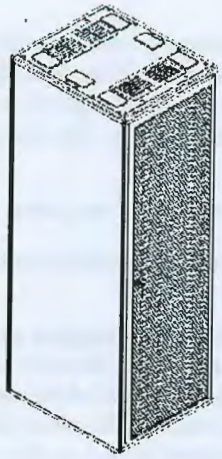
Step 5. Attach the bezel to the front of the server. The cabinet-mounted server will now look like the picture shown below.

Installation In Third-Party Racks

Overview

HP has qualified the rack systems of several vendors as suitable for rp24xx server installation.

To qualify each rack configuration, specific rack vendors and rack products have been identified. Each vendor has several rack product lines. rp24xx servers are supported only in HP cabinets or in qualified vendor racks, as shown below:



Examples of cabinets are Chatsworth (CPI) Megaframe, Wrightline Paramount, Rittal Vario, Vero IMRAK, SMC, Zero Express Rack and Bud Industries S2000. For further information, refer to the table titled, *Third Party Rack Ordering Guide for Vendor Products*, at the end of this section.

Third Party Rack Checklist for rp24xx Server Installations

This document is a guide to insure safe and reliable installation and operation of rp24xx servers in third party EIA-style racks and applies to installations at the end-customer site only.

Footprint

The rp24xx server is 25 inches deep. Additional space for cable management is required in the rear. HP recommends 40 inches in front and 24 inches in the rear for service access and proper safety in proximity to energized electronic equipment.

Safety Checklist

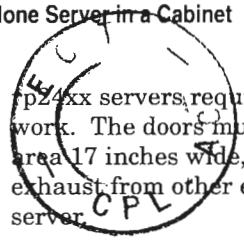
To insure the installation is safe, the following items must be addressed:

Anti-tip safety	The rp24xx server slides out of the rack about 24 inches for service. When extended this far, there can be a major tip hazard for the rack. If the rack has anti-tip feet front and rear, attach them prior to installing the server. If anti-tip feet are not available, ensure that the rack is solidly bolted to the floor both front and rear. Ensure that the thick sheet metal of the rack base provides for a bolt-down bracket.
Rack slides	When servicing the HP rp24xx server, it is critical to use properly attached rack slides, which will allow the detents to stop the sliding motion of the unit. Always work on the server when it is fully extended and locked in place to avoid injury to maintenance personnel.

Warranty Checklist

The following factors must be considered to insure that HP's warranty is valid in third party rack configurations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 654
3698
Doc.



Air flow

rp24xx servers require front-to-back airflow. Therefore, a solid front or rear door will not work. The doors must be removed or changed to a 63% open perforation pattern over an area 17 inches wide, top to bottom, minus a 2 inch border. Also insure that the hot air exhaust from other equipment is not being presented to the intake (front) of the rp24xx server.

Service Access

To insure that the rp24xx server can be serviced properly, the installation must allow for a free sliding distance of 40 inches out the front of the rack. This will also allow HP to use the standard service contract for any rp24xx server in the field regardless of the racking situation. Alternate service contracts are addressed later in this document.

Cable strain relief

The cable management solution for the rp24xx server is in two parts:

1. There is a wire-form cable management system that attaches to the rear of the server that provides a strain relief attachment point.
2. The cable bundle from each server must be Velcro tie-wrapped and fed into a 40 inch service loop. The service loop allows the server to slide forward completely out of the rack for access. For warranty purposes, a proper method of strain relief must be used, especially for any SCSI-type cables on the PCI cards. This may force the elimination of the rear door in some cases. Judgement is required based on the following examples:

- MINIMAL CABLING- If the customer has a power cable and two LAN cables attached to the rp24xx server, cabling options include an alternate strain relief system, to allow the rear door (if perforated) to be used for security.
- FIBER OPTICS CABLING – Fiber optics cable allows a 1.5 inch bend radius and has a very low profile connector. Fiber optics cable bundles are relatively small and can be held to the inside of the wire-form strain relief.
- MAXIMUM SCSI CABLING – If ultra-flex SCSI cables are used, the bend radius allowable is 1.5 inches with a low profile connector. the customer must use the provided wire form strain relief parts. HP strongly recommends using a server rack that provides the extra space required to house excess cabling.

rp24xx server PDU Support

PDUs for rp24xx servers must be ordered as separate products when configuring a Third Party Rack order.

The PDUs are:

Table 0-2

E7674A 19"	16A	100-240V
E7681A 19"	30A	100-240V
E7682A 19"	60A	100-240V

Supportability Matrix

The following table shows supportability requirements.

Table 0-3

Major Features	rp24xx server w/ Full HA

Table 0-3 (Continued)

Anti-Tip	MUST
Proper slides	MUST
Airflow	MUST
Service Access	MUST
Cable Strain Relief	MUST
Front Access	40 inches
Rear Access	24 inches

Third Party Rack Ordering Guide for Vendor Products

Table 0-4

Rack	Mounting Hardware	Doors	Qualified Tip Stability Device	Contact
Chatsworth Megaframe Rack (cabinet)	12468 Series Full Rack Mounting Rail, pair[a] 12464 Series Half Rack Mounting Rail, pair[a]	14032 Series Perforated Metal Door	712441-001 Floor Clamp Kit	www.chatsworth.com

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 655
Doc.

Table 0-4 (Continued)

Rack	Mounting Hardware	Doors	Qualified Tip Stability Device	Contact
Wrightline Paramount Frame 40" Deep JF842440	JRK44190 Rail Kit and JHP0N001 rp24xx server Adaptor Bracket	JDF8242L Paramount 84" x 24" left-hinged JDF8424R Paramount 84" x 24" right-hinged JDP84242 Paramount Frame perforated door insert for 84" x 24" door frame JTPP2440 perforated top panel - 24"W x 40"D	Floor anchoring	www.wrightline.com
SMC 36" Deep LAN Storage Module	rp24xx server Adaptor	Ventilated Front and Rear	Floor anchoring	Sales & Customer Support 1-800-SMC-PLUS (1-800-762-7587)

a. Requires purchase of two.

NOTE For additional or other third party rack vendor product information, contact the HP Enclosures Technical Marketing Manager at (408) 873-6692.

Server Slide Rail Installation

The following information contains instructions for installing rp24xx servers in a cabinet.

CAUTION Both anti-tip feet must be properly affixed before installing equipment in a cabinet on a slide assembly.

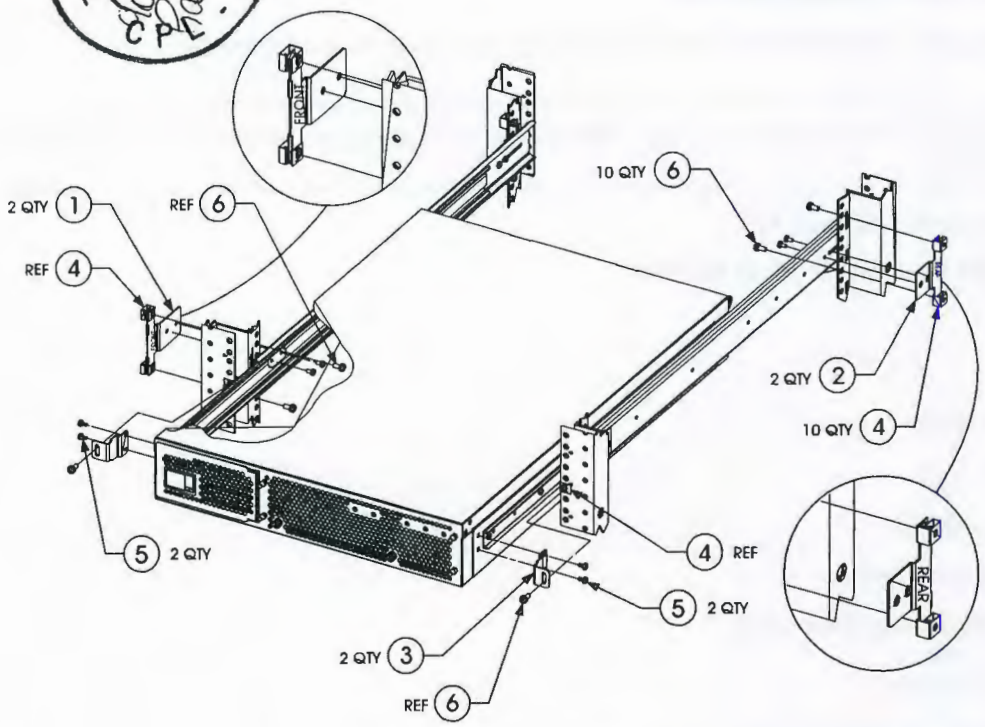
Tools needed: Torx Drivers, T15 and T20.

Slide Rail installation kit contents are as follows:

2	Slides, inner
2	Slides, outer
2	Slides mount, front
2	Slides mount, rear
2	Plastic bezel end caps
1	Cable Management device
1	see-through plastic bag containing: 2 bracket end caps 2 rack mounting ears
1	see-through plastic bag containing: 2 front RBI adapters 2 rear RBI adapters 2 cres fr flanges 4 M4 x 0.7 screws 10 10/32 x 0.5" screws 10 Sheet metal nuts (Note: Contains non-E-series HP cabinet hardware, also)
1	see-through plastic bag containing: 4 plastic snap rivets 4 sheet metal nuts 8 M5 screws 16 M4 screws

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº
3698
Doc.

The following illustration shows rail parts only. Plastic parts bags, plastic end caps, and the cable management device is not shown.



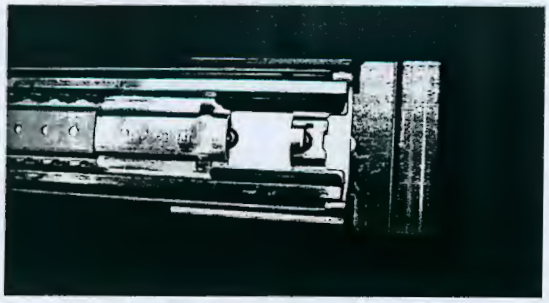
RACK KIT ASSEMBLY

ITEM	QTY	PART/MATERIAL-DESCRIPTION	PART NUMBER
6	10	SCREW, 10-32 x 0.5 INCH	2680-0278
5	4	SCREW, M4 x 0.7mm	0515-2478
4	10	SHEET METAL NUT	0590-0804
3	2	FLANGE	A5570-00044
2	2	ADAPTER, REAR	A5570-00043
1	2	ADAPTER, FRONT	A5570-00042

NOTE This illustration shows non-E-series HP cabinet columns

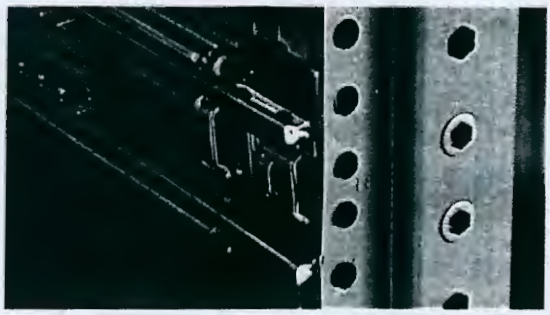
The following procedures list the steps required to install a stand-alone server in a cabinet.

Step 1. Attach rear slide mounts to the outer rails using M4 x 0.7mm screws. Do not fully tighten screws. Allow the rear slide mount to move along slot in the outer rail.



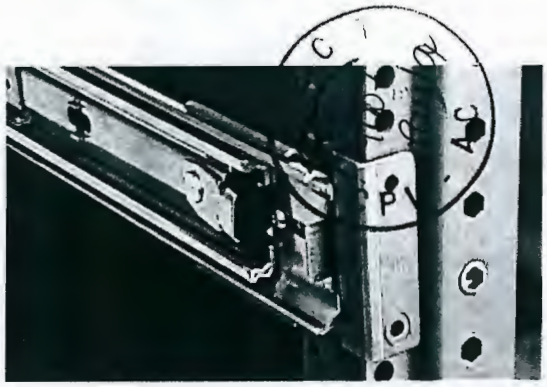
Step 2. Place the outer rails with mounting brackets in the rack. Engage support hooks in the rack columns. The front mounts and rear mounts are different, as shown below:

Support Hook attached to rack column.



Front Slide Mount Placement

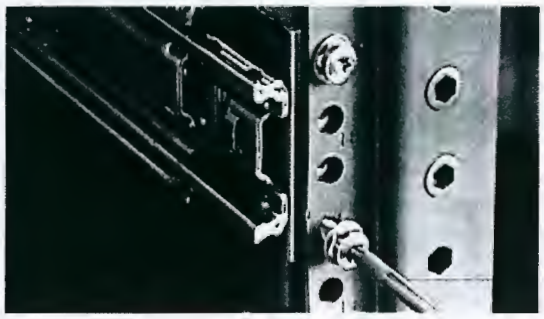
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 657
Doc.



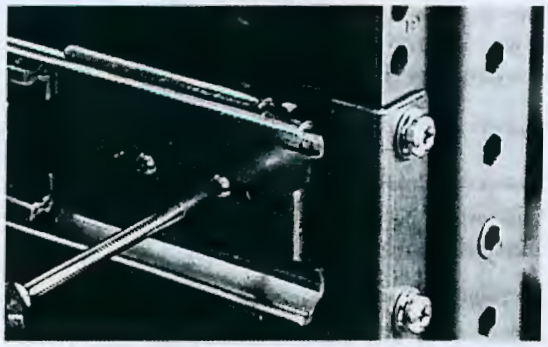
Rear Slide Mount Placement

Step 3. Install sheet metal nuts on rear columns. Locate the slide mount laterally against rack column. Install and tighten the M5 x 0.8mm machine screws.

Step 4. Install and tighten the M5 x 0.8mm machine screws on the front slide mounts.



Step 5. Tighten the M4 x 0.7mm screws that attach the slide rails to the rear mounts.



Step 6. Locate and install the inner slides on the sides of the server, using M4 x 0.7mm machine screws. The inner rails contain a flat spring latch. The free end of the latch goes toward the front of the server, the riveted end goes toward the rear of the server chassis.

Step 7. Double-check all mounting screws to ensure that they are tight.

Step 8. Completely extend both outer slides to the front of the rack. Outer slides should latch in the extended position.

Step 9. Align the inner rails on the server between the extended outer rails on the rack.

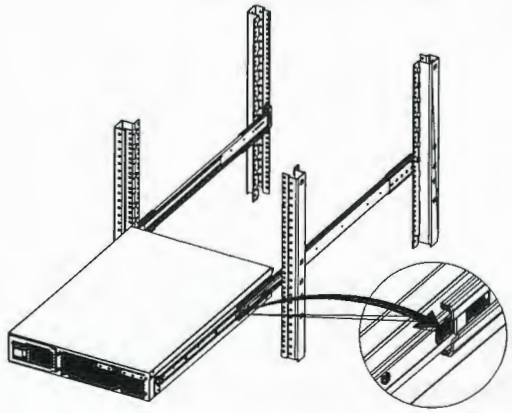
WARNING **The rp24xx server weights 22.68 kg (50 lbs). Use two people or a lift during installation. Take necessary precautions to prevent muscle strain when lifting or carrying the server.**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 658
Doc.

Do not lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency. Failure to heed this warning may result in personal injury and/or permanent damage to the server

NOTE The rail sets on both sides of the chassis must be properly aligned and engaged before attempting to slide the server into the cabinet.

The inner rail (attached to the server) must have *both* top and bottom edges *inside* the outer (cabinet) rails

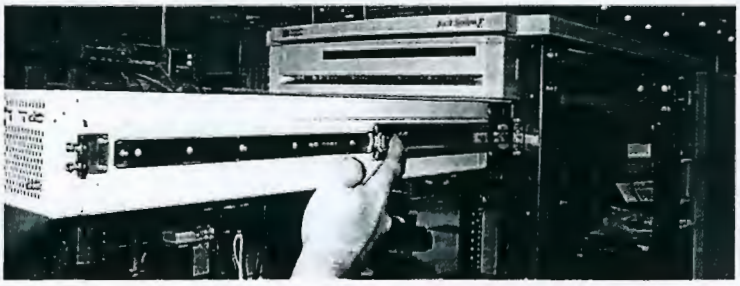


ecrr014

Step 10. Carefully guide the inner slide rails on the server chassis into the outer rails, engaging the ball bearing carriers.

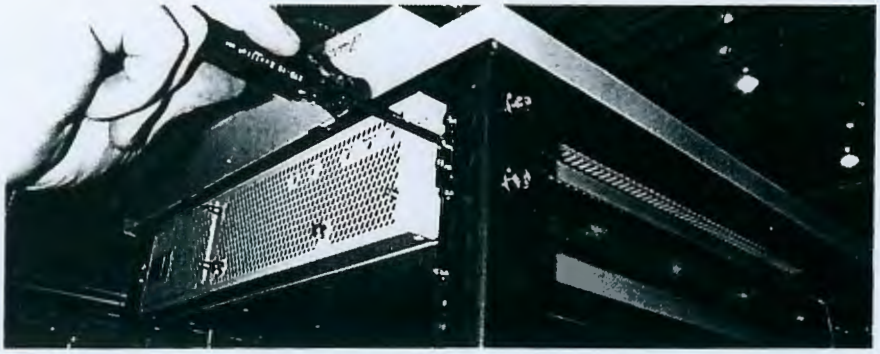
CAUTION Do NOT force the slides together. To do so may damage the ball bearing carriers. The inner slides will latch after travelling a few inches.

Step 11. Press the slide latches on the inner slides and carefully slide the server completely into the rack.

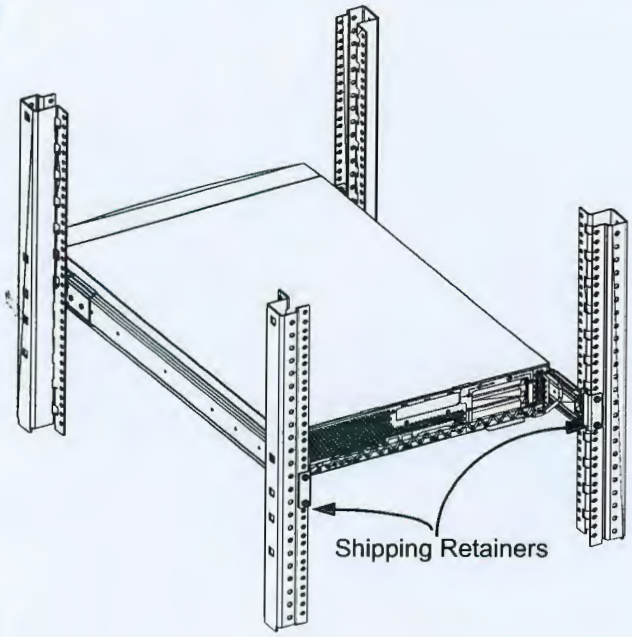


Step 12. Verify operation of the slides and check alignment of the server in the rack.

Step 13. Secure the server to the rack columns with M4 x 0.7mm screws and M4 clip nuts.



Step 14. Optional: Install shipping retainers at the rear of the unit if the server is to be shipped while installed in a rack. Install retainers with M5 x 0.8mm screws and M5 clip nuts.



ccrr013

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 659
Doc.

Cabinet Installation

Installation of a factory-loaded cabinet consists of the following steps:

Step 1. Move the cabinet to the installation site.

Step 2. Lower the leveling feet. (This will prevent excessive wear on the casters, level the cabinet, and provide stability.)

WARNING **Extend or install the cabinet stabilizers, located at the bottom of the front of the cabinet, as an additional safeguard against the cabinet toppling forward during installation.**

Failure to observe this precaution could result in personal injury or death and equipment damage.

Step 3. Connect the console and system peripherals to the server(s).

NOTE Attaching cables while the rails are extended fully forward will ensure that sufficient slack is available for later maintenance.

Step 4. Connect the cabinet power cord to the appropriate wall outlet.

Step 5. Be sure all peripherals outside the cabinet are connected to wall outlets.

The cabinet/server system assembly is now ready for the power up process.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 660
Doc.

Cabinet Mounted Server Unpack

Overview

rp24xx servers can be procured in two modes: stand-alone or pre-installed in a cabinet at the Hewlett-Packard factory. Stand-alone servers can be installed in an existing HP-supported cabinet by purchasing Rail Kit A5810A.

Installing a Factory-integrated Cabinet

Unpacking the Cabinet

NOTE It is the customer's responsibility to inspect the shipping package for damage.

It is the Hewlett-Packard Customer Engineer's responsibility to remove the cabinet assembly from the shipping pallet.

WARNING **A fully configured 2.0 meter cabinet can weigh over 500 kg (1100 lbs). Be careful not to tip the cabinet while unpacking.**

Failure to heed this warning can result in serious injury or death and equipment damage.

To unpack the cabinet, perform the following steps:

WARNING **Wear protective glasses while cutting the plastic bands around the shipping container. These bands are under tension.**

Failure to heed this warning can result in serious eye injury if the severed bands snap back and hit you in the face.

Step 1. Cut the plastic polystrap bands around the shipping container.

Step 2. Follow the procedure listed below to prepare the cabinet for removal from the pallet:

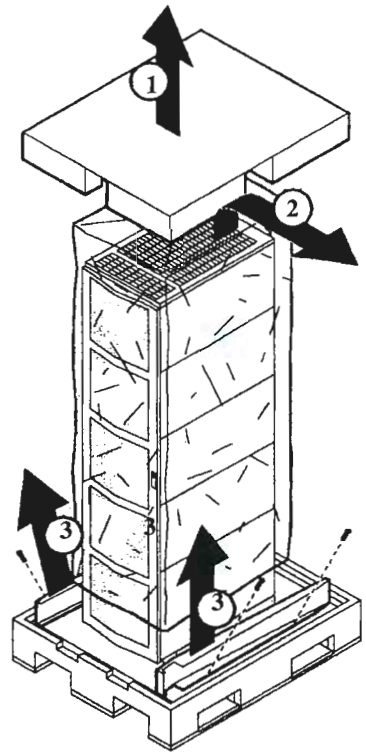
a. Lift the cardboard top cap off of the shipping box (callout 1).

b. Remove the packing material underneath the cap (callout 2).

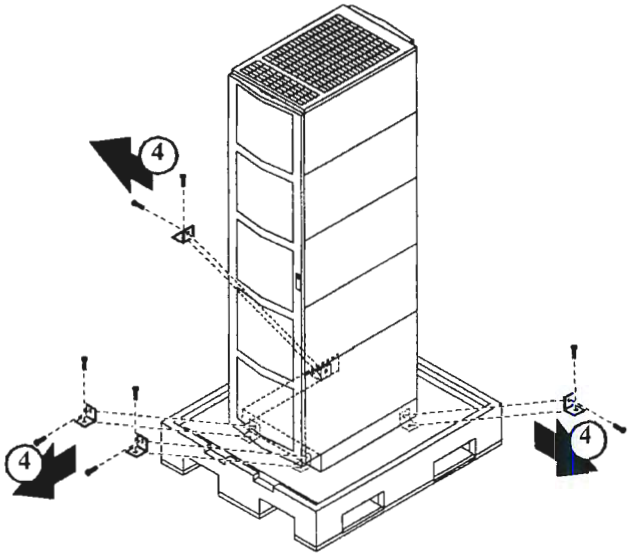
c. Remove the clamshell box and place out of the way.

d. Remove the screws that secure the ramps in place and lift the ramps out (callout 3).

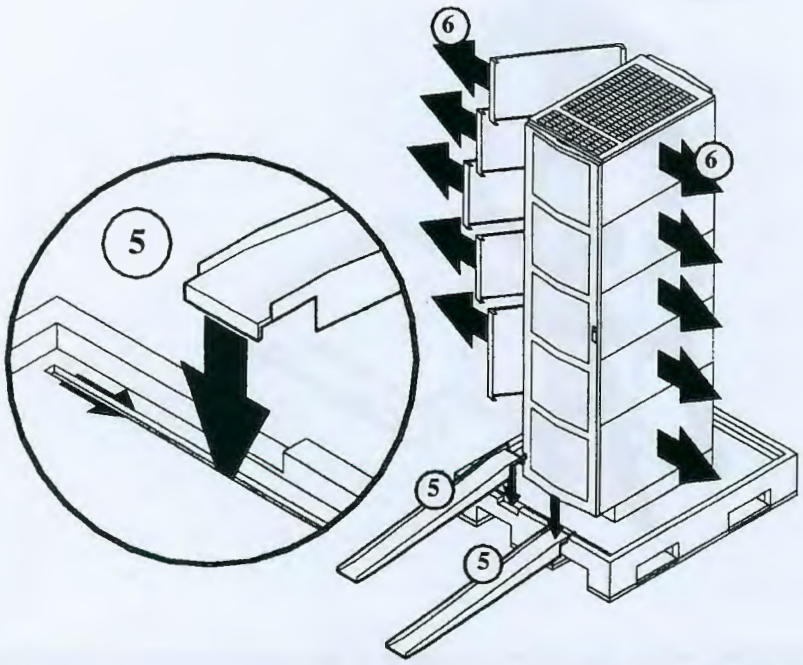
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 661
Doc. 3698



Step 3. Remove the brackets securing the cabinet to the pallet (callout 4).



Step 4. Insert the ramps in the notches provided on the pallet (callout 5). Remove the side panels from the cabinet and set them aside (callout 6).

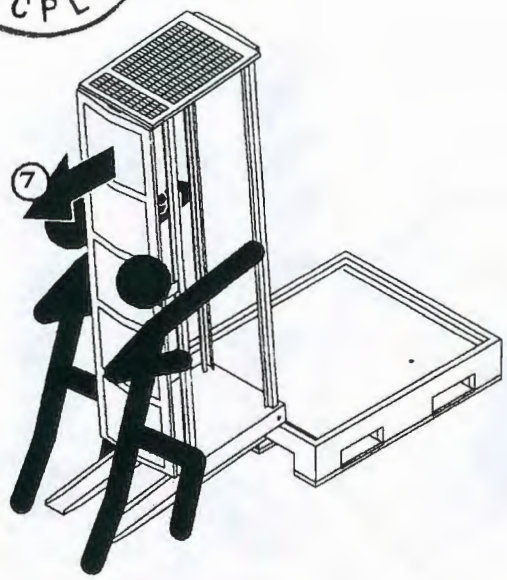


WARNING: A fully configured 2.0 meter cabinet can weigh over 500 kg (1100 lbs). Always use at least two people to roll the cabinet off of the pallet. Be careful not to tip the cabinet while unloading.

Failure to heed this warning can result in serious injury or death and equipment damage.

Step 5. Use at least two people to roll the cabinet off of the pallet and down the ramp (callout 7).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 662
Doc. 3498



Cabinet Inspection

Once the cabinet is off the shipping pallet, but before moving it to the installation site, inspect the internal and external condition of the cabinet.

Cabinet Exterior Checklist

Check the cabinet exterior for signs of shipping damage:

- ❑ Look at the top and sides for dents, warpage, or scratches.
- ❑ Check the server front bezels for alignment, scratches and breakage.
- ❑ Check any filler panels on the front of the cabinet for proper fit.
- ❑ Check the rear door for dents, scratches, proper fit when closed, and operation.

Cabinet Interior Checklist

Open the rear door and inspect the inside of the cabinet:

- ❑ Inspect all cables and ensure that they are secure.
- ❑ Inspect all rails for signs of damage.
- ❑ Check all mounting screws for tightness.
- ❑ Check all components for signs of shifting during shipment or any signs of damage.

NOTE If the shipment is either incomplete, damaged, or fails to meet specifications, notify the nearest Hewlett-Packard Sales and Support Office. If damage occurred in transit, notify the carrier as well. Hewlett-Packard will arrange for replacement or repair without waiting for settlement of claims against the carrier. If the shipment was damaged in transit, keep the shipping containers and packaging material for inspection. If extensive damage is found, it may be necessary to return the entire cabinet to HP.

PowerTrust Uninterruptible Power Supply (UPS) Option

Unpack the PowerTrust UPS and use the installation information in the *PowerTrust System Guide,* included with the UPS, to connect the UPS to the cabinet.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 665
Doc. 3698

ECT
Paula
AC

Repackaging the Cabinet for Shipment

Use the original packing material to repackage the cabinet for shipment. If the packing material is not available, contact your local Hewlett-Packard Sales and Support Office regarding shipment.

Before shipment, place a tag on the container (or equipment) to identify the owner and the service to be performed. Include the equipment model number and the full serial number, if applicable. The label showing the model number and the full serial number is located on the outside of the rear door.

Due to the weight of a fully loaded cabinet, it will require two people to push the cabinet up the ramp onto the pallet.

WARNING: Repackaging a loaded cabinet may be hazardous because a fully configured 2.0 meter cabinet can weigh up to 500 kg (1100 lbs). Always use two people when moving the cabinet and when positioning the cabinet on the pallet. Check the condition of the loading/unloading ramp before use. If the ramp appears damaged, DO NOT attempt to push a loaded cabinet up the ramp onto the pallet. Contact your local Hewlett-Packard Sales and Support Office regarding shipment. Failure to heed this warning can result in serious injury or death and equipment damage.

To repackage the cabinet, follow the repacking checklist and refer to the unpacking instructions for detail.

Repacking Checklist:

- ❑ Assemble the HP packing materials that came with the cabinet.
- ❑ Connect the loading ramp to the pallet.
- ❑ Raise the cabinet levelers before moving the cabinet.
- ❑ Retract or remove the stabilizers.
- ❑ Push the cabinet up the ramp onto the pallet. Be sure to position the cabinet so that the front goes up the ramp first.
- ❑ Secure the cabinet to the pallet with the shipping clamps, shipping block, and rear door support.
- ❑ Place the anti-static bag over the cabinet.
- ❑ Place bezel support packing on the front corners of the cabinet. Secure it with a wrap.
- ❑ Place the top cap packing material and loading/unloading ramp on top of the cabinet.
- ❑ Wrap the clam shell box around the cabinet.
- ❑ Put the box top on the box and secure the assembly to the pallet.

Be sure to follow the tagging and labeling instructions mentioned earlier. The cabinet is now ready for shipment.

EBS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 664
Doc. 3698

Stacking Servers

Stacking Servers

Hewlett-Packard will support stacking up to six rp24xx servers if the following conditions are met and the correct procedure followed.

NOTE HP will not support the stacking any other A-Class server.

CAUTION In order to remain within weight limitations and to prevent tipping, do not stack servers more than six high. Each server weighs approximately 23 kg (50 lbs). DO NOT lift more than one server at a time.
Always use the strap when stacking servers, regardless of the number. Hewlett-Packard will not support or warrant servers that are damaged as a result of being improperly strapped or stacked more than six servers high.

Follow the steps listed below:

Step 1. Remove the rubber "feet" from the packing material and place one rubber foot squarely on each of the four corners on the bottom of each server.

Step 2. Lay the enclosed binding strap out flat and straight.

WARNING **DO NOT attempt to lift the server by the front bezel. The plastic bezel is attached by pressing it onto four ball-tipped posts located on the front of the server cover and pulls off with very little pressure.**

The bezel WILL NOT support the 23 kg (50 lb.) weight of the server.

Failure to observe this precaution will cause damage to the server and may cause personal injury.

Step 3. Place the first server over the strap and position the strap so that it can be firmly cinched down on the top server.

Step 4. Carefully set the remaining servers (up to five) on top of the first server so that the four feet of each of the remaining servers are squarely on the top of the server below.

WARNING **Do not cinch the strap so tightly that the chassis buckles.**

Failure to heed this precaution may cause internal components to be damaged and/or the server cover may not seat correctly to seal the server from dirt and dust.

Step 5. Center the strap midway between the front and rear of the stack and pull the ends up over the top server. Thread the flat end through the loop end and pull it snug. Press the Velcro® pieces together firmly and lay them flat on the top cover of the top server.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 665
Doc. 3698

CAUTION DO NOT stack heavy objects, such as monitors, on top of the server. The weight may cause the top to cave in and damage internal components.

ECT
8988
Paula
CPL - AC

5 Operating Instructions

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 667
3698
Doc.

ECT 8987 Fls CPL - ACI

Configuring the Guardian Service Processor (GSP)

The Guardian Service Processor (GSP) is resident in the system to allow the system administrator to monitor and perform administrative functions locally on the system console, or at a console in another area. This section provides configuration procedures that will:

- Configure the GSP Local Area Network (LAN) port
- Add or delete GSP users (maximum of 20)
- Change the default GSP configuration.

Configuring the GSP LAN Port

Perform LAN configuration from the system's local port (either console or the HP secure web console).

NOTE The GSP LAN port is different from the System LAN. It will need a separate:

- 10BaseT LAN connection
- Subnet mask
- Gateway address
- Hostname (to be used when messages from the console are logged or printed)

To configure the GSP LAN port, perform the following steps:

Step 1. To select the GSP, enter: **ctrl + b**.

Step 2. At the GSP prompt, enter the following LAN Configuration (lc) command:

```
GSP> lc
```

The *lc* comrp24xxmand will start a series of prompts. Respond to each prompt with the appropriate information.

Adding Users

The GSP stores access information for a maximum of 20 users (one administrator and 19 operators). By design, the first user entered into the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users, or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

To add a user, perform the following steps:

Step 1. Type **ctrl + b** to access the GSP.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls Nº 668 3698 Doc.

Step 2. At the GSP prompt, enter the Security options and access control (SO) command:

```
GSP> so
```

Step 3. The first prompt you will see with the *so* command is for the following GSP-wide parameters:

- Login Timeout: 1 minutes.
- Number of password Faults allowed: 3.
- Flow Control Timeout: 5 minutes.

The terminal will then display:

```
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

Enter **Y** to modify GSP-wide parameters, or enter **N** to continue to add users.

If you enter Y, the parameters will be displayed in an edit mode to allow modification.

If you enter N, continue to the next step.

NOTE The first user entered (user number 1) is identified as the GSP administrator.

If you are adding users, you will need to step through all current user entries to reach the next available user prompt.

Step 4. The terminal will display:

```
Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __
```

Enter **Y** to modify user number 1 parameters, enter **N** to leave user number 1 parameters unchanged or enter **Q** to quit and return to the GSP prompt.

If you enter Y, the parameters will be displayed in an edit mode to allow modification.

If you enter N, the terminal will display:

```
Do you want to modify the user number 2 parameters? (Y/[N]/Q to quit) __
```

Enter Y, N, or Q and proceed according to the instructions shown above in this step.

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry could deny entry to that user.

The following list is an example of added users information:

User's Name: Joe Smith
Organization's Name: IT Support
Dial-back configuration: Disabled
Access Level: Operator
Mode: multiple
User's state: enabled

For the number 1 user, the Access level is administrator.
A Mode entry of single only allows entry for that user one time, after which, further logon attempts are denied and the user state is set to disabled.
A Mode entry of multiple allows unlimited logon access to the GSP for that user.

Removing Users

You can remove (disable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

Step 1. Enter **ctrl** + **b** to access the GSP.

Step 2. At the GSP prompt, enter the Security options and access control (SO) command:

```
GSP> so
```

Step 3. The first prompt you will see with the *so* command is for the following GSP-wide parameters:

- Login Timeout: 1 minute.
- Number of password Faults allowed: 3.
- Flow Control Timeout: 5 minutes.

The terminal will then display:

```
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

Enter N and continue to the next step.

NOTE You may need to step through several user numbers until you reach the user to be removed.

Step 4. When you access the number of the user to be removed, modify the User's state to *Disabled* and change any other user information necessary.

Changing the Default GSP Configuration

This section describes the process of changing GSP default configuration to the default (factory preset) values. To reset the GSP to its default configuration, perform the following steps:

Step 1. Enter **ctrl** + **b** to access the GSP.

Step 2. At the GSP prompt, enter the Default Configuration (dc) command:

```
GSP>co
```

Step 3. Follow the prompts to change all GSP configurations to the default values.

CAUTION When the Security configuration is reset using the *GSP>dc* command, all users, including the GSP administrator, are removed *Remote* is disabled, and the network configurations are reset to the factory default values. The *Remote* functionality must be re-enabled through the main console using the Enable Remote (er) command. The IP address, hostname, subnetmask, and the gateway IP must be re-entered through the main console using the *LAN Configuration* (lc) command.

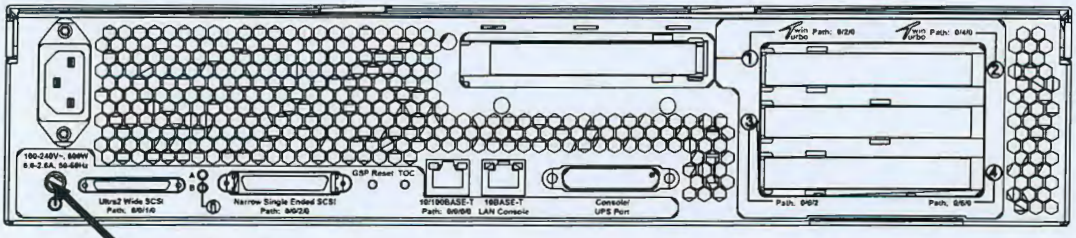
RQS nº 03/2005 - CN
CPMI - CORREIOS
0669
Fls. Nº
3698
Doc.

8983 Paula
CPI AC

Initial Power-up

The following section describes the process of applying power to the server and booting the system to the operating system Login prompt.

1. Apply AC Power to the system console.
2. Apply power to the server by pressing the rear panel On/Off switch IN.



ccrr012

3. A series of self-test boot progress messages will scroll rapidly up the screen. Some messages may pause for up to one minute while the test completes.
4. The initial power-up selftest process will complete in one to five minutes and the Boot Console Handler (BCH) main menu will be displayed.
5. To start the boot process using the primary boot path, type *BO PRI*, at the BCH main menu prompt and press **ENTER**.

NOTE Booting a system to a operating system login prompt from BCH main menu can take 20 minutes or longer depending on your software and hardware configuration.

6. Once the system reaches the operating system login prompt, a display similar to the following will be shown on the console screen:

```
HP-UX hprtos A.09.04 U 9000/897 (ttyp2)

login:
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 670
3698
Doc.

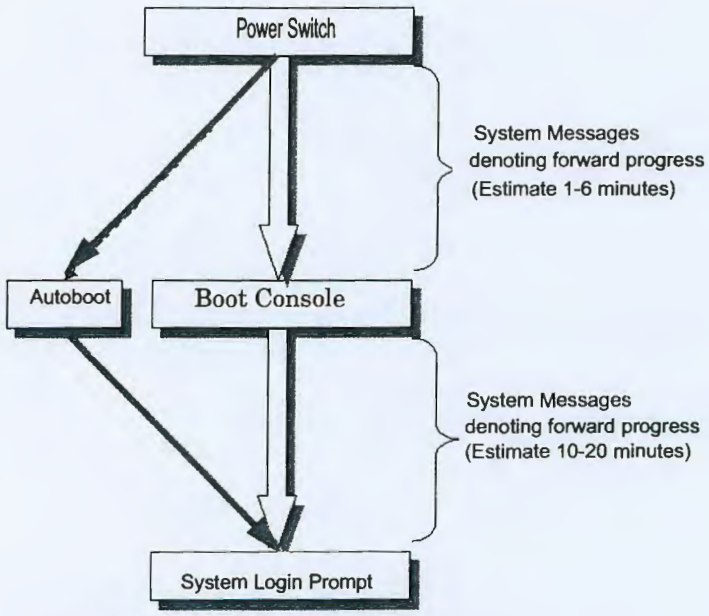
ECT 8981 C. Paulista AC L I

Boot To Operating System

The length of time required to boot the system depends on the number of processors and the amount of RAM memory installed. Average configurations can take 20 minutes or more.

The boot process is shown in the following illustration:

Typical Boot Process



The duration of the full boot process can vary depending on:

- Number of CPUs installed
- Amount of Memory installed
- Operating System version installed
- State of the network

(Total time to boot will vary)

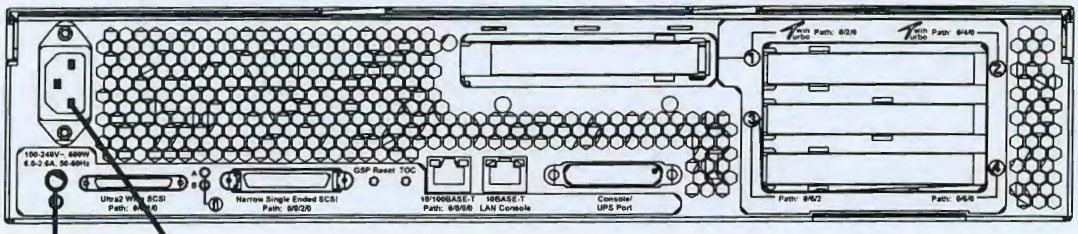
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 671
3698
Doc.

System Power Down

1. Stop all active applications that may be running and Log Off all users.
2. Perform a system backup of the entire Operating System and data base. If this is not feasible, perform a backup of the data base. (Backups should be performed at a scheduled interval as common practice for protecting any new data or changes to the existing data base.)
3. To shut down the OS, enter, "`/etc/shutdown -h`" at the prompt.
4. At the rear of the computer, press and release the on/off switch to power-down the server.

NOTE Housekeeping voltage is still present after switching power off. Unplug the power cord to completely remove power.

5. Unplug the power cord from the server.



Power Cord Receptacle

On/Off Switch

ccrr012

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 672
Doc. 3698

8977
Paula
CPL - AC

6 Adding Components to the Server

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 673
3698
Doc.

Add Memory

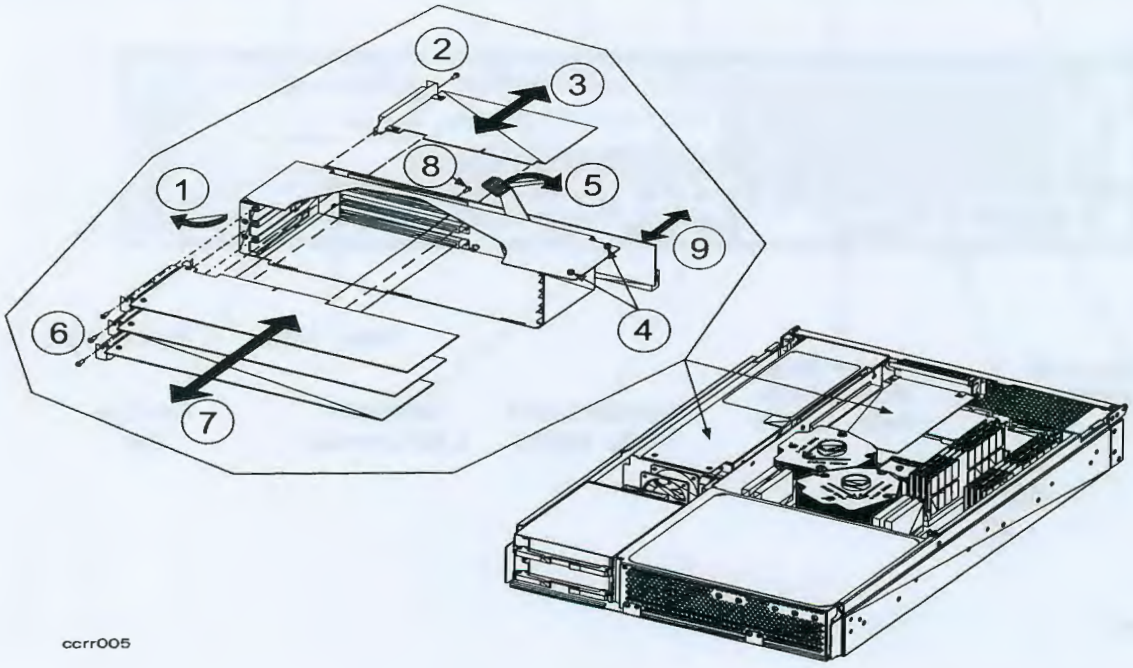
Memory Configuration Rules

rp24xx servers have 8 slots (4 DIMM pairs) on the system board for memory DIMMs. These slots are numbered 1through 8. Four slots (5 - 8) are disabled on A400 servers. A500 servers can access all slots. The following rules govern the installation of memory DIMMs:

- Memory must be installed in DIMM pairs.
- The capacity of DIMMs within a pair must be the same.
- Install DIMMs with the greatest capacity in the lowest slot numbers.
- Install DIMMs in numerical order starting with slot 1 (1, 2, 3, etc.).

Add Peripheral Component Interconnect (PCI) Cards

rp24xx servers have a total of 4 PCI I/O slots. Slot 1 is short slot, located outside the I/O card cage, connected to the back of the I/O Backplane. Slots 2 through 4 are located inside the I/O card cage. Slots 1 and 2 are Twin Turbo slots; slots 3 and 4 are Turbo slots.

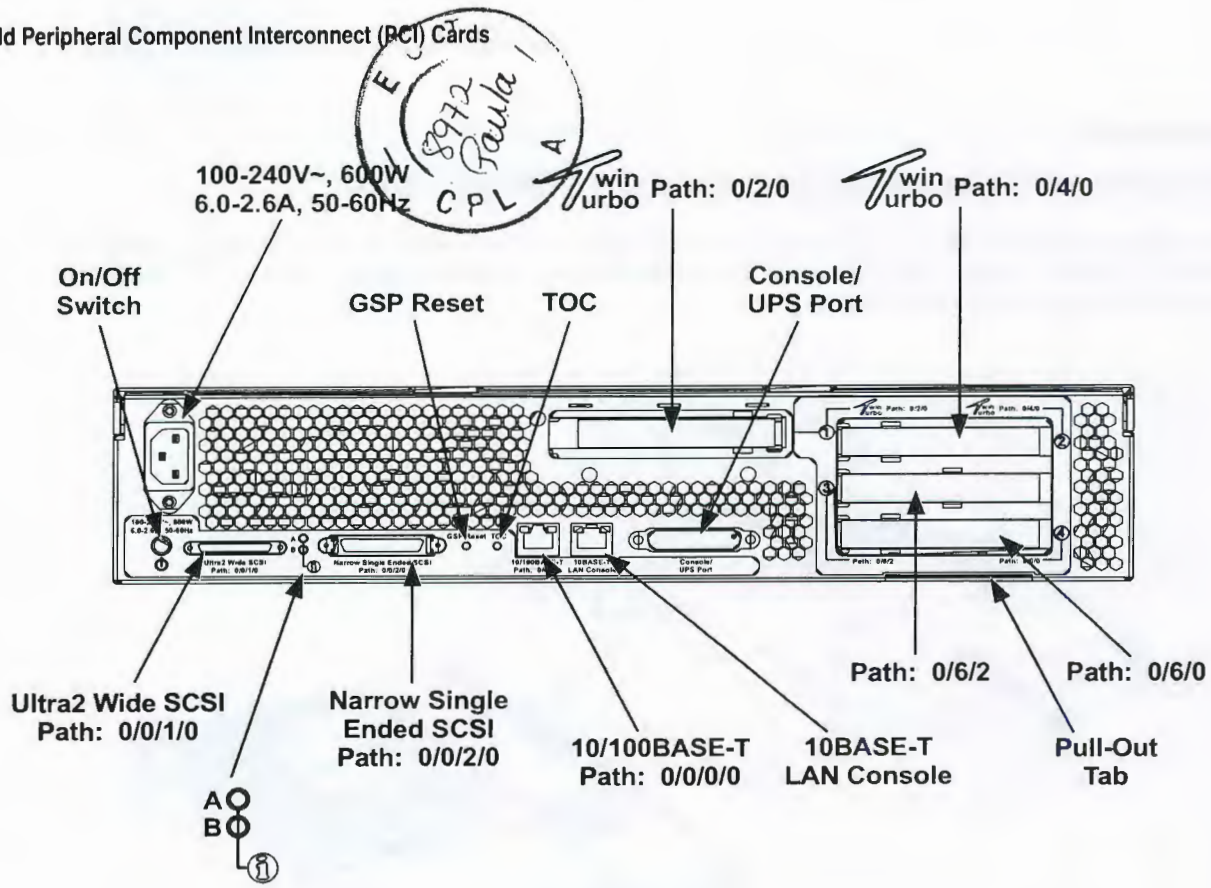


ccrr005

No.	Name	No.	Name
1	I/O Card Cage	6	I/O Card anchor screws
2	Outside I/O Card anchor screw	7	I/O Cards #2 through #4
3	Short I/O Card #1 (may be Secure Web Console)	8	I/O Backplane anchor screw
4	I/O Card Cage anchor quarter-turn fasteners	9	I/O Backplane
5	I/O Backplane disconnect lever		

- Slots 1 and 2 are Twin Turbo slots. Each Twin Turbo slot has a dedicated PCI bus and supports 32 and 64-bit PCI cards.
- Slots 3 and 4 are Turbo slots. They share a single PCI bus and support 32 and 64-bit PCI cards.

A400 servers have access to slots 1 and 2 only. A500 servers have access to all four slots. The following graphic shows the PCI slots on the rear of the server, right side.



ccrr008

New I/O Cards For rp24xx

The following table lists new I/O cards for the rp24xx.

NOTE The first HP-UX release for the new cards is 11.00.

I/O Card No.	Description
A6828A	U160 Single Port SCSI
A6829A	U160 Dual Port SCSI
A6795A	2Gb, Single Port Fiber Channel LAN
A6825A	1000BaseT Next Generation LAN
A6847A	1000BaseSX Next Generation LAN
A6386A	Hyperfabric2 (HF2) Clustering

These cards can be used in addition to the legacy cards shown below.

The following HP-UX restrictions apply regarding the installation of PCI I/O cards that contain a PCI-to-PCI bridge:

- HP-UX boot is currently not supported for cards that contain a PCI-to-PCI bridge.
- HP-UX patches are required when more than one card containing a PCI-to-PCI bridge is installed in shared slots (slots #3 and #4).

PCI cards are installed in the factory as shown in the Load Order column below, beginning with slot 1. Use the following table as a guideline for installing PCI I/O cards in the field. A system shipped from the factory may have a different configuration than one built in the field.

NOTE: All cards are not supported by A4 operating systems.

Load Order	Product Number	PCI Card Description	Part #	Max.	Boot	Future Rel.	Notes
1	A4926A	Single Port 1000BaseSX Gigabit Ethernet LAN (H)	A4926-60001	4	No	x	
2	A5483A	ATM 622 (MMF connector (H)	A5483-60001	4	No	x	
3	A6092A	Hyperfabric (H)	A6092-60001	4	No	x	
4	A4929A	Single Port 1000baseT Ethernet LAN Adapter (Gigabit ethernet copper) (H)	A4929-60001	4	No		
5	A5838A	Dual port 100baseT/X/dual port Ultra 2 SCSI Combo Interface card (F)	A5838-60001	1	No		1
6	A5506B	Quad Port 10/100B-TX LAN (F)	A5506-60101	1	No	x	1
7	A5856A	RAID Card (F)	A5856-60001	1	No		1
8	A5513A	ATM 155 (MMF connector) (H)	A5513-60001	4	No	x	
9	A5515A	ATM 155 (UTPS connector) (H)	A5515-60001	4	No	x	
10	A4800A	Single port Fast/Wide/Diff. SCSI-2 (H)	A4800-62002	4	Yes		4
11	J3525A	Dual Port serial (X25/FR/SDLC) (H)	J3525-60001	4	No		
12	A5158A	Single port Fibre Channel 1062Mb/s (H)	A5158-60001	4	Yes		
13	A5783A	Token Ring (4/16/100 Mb/s) (H)	A5783-60001	4	No	x	
14	A5230A	10/100B-TX LAN (RJ45) (H)	B5509-66001	4	No		
15	J3592A	8 Port Terminal MUX (H)	J3592-60101	4	No	x	
16	A3738A	Single Port 10/100B-TX (AUI, BNC, RJ45) (H)	A3738-60001	4	No	x	
17	J3593A	64 Port Terminal MUX (H)	J3593-60001	2	No	x	

ROS 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 676
Doc.

Load Order	Product Number	PCI Card Description	Part #	Max.	Boot	Future Rel.	Notes
18	A3739B	FDDI Dual Attach Station LAN Adapter (H)	A3739-60002	4	No		
19	A5150A	Dual Port Ultra2 SCSI (F)	A5150-60001	3	Yes	x	4
20	A5149A	Single port Ultra-2 SCSI Interface card (F)	A5149-60001	3	Yes		4
21	A5486A	Public Key Cryptography (PKC) PCI (F)	A5486-60001	3	No	x	
22	A5159A	Dual Port FWD SCSI-2 (F)	A5159-60001	3	Yes	x	4
23	J3526A	Quad Port Serial (X25/FR) (F)	5063-1322	3	No	x	
24	A5858A	Secure Web Console PCI Card (H) (Optional)	A5858-70001	1	No		2
25	A6150	PCI 2D Graphics and 2 part USB adapters (H)	A6150-60001/ A6150-60002	1	No		3
(F) = Full length I/O card -- (H) = Half length I/O card. NA = Not Applicable							

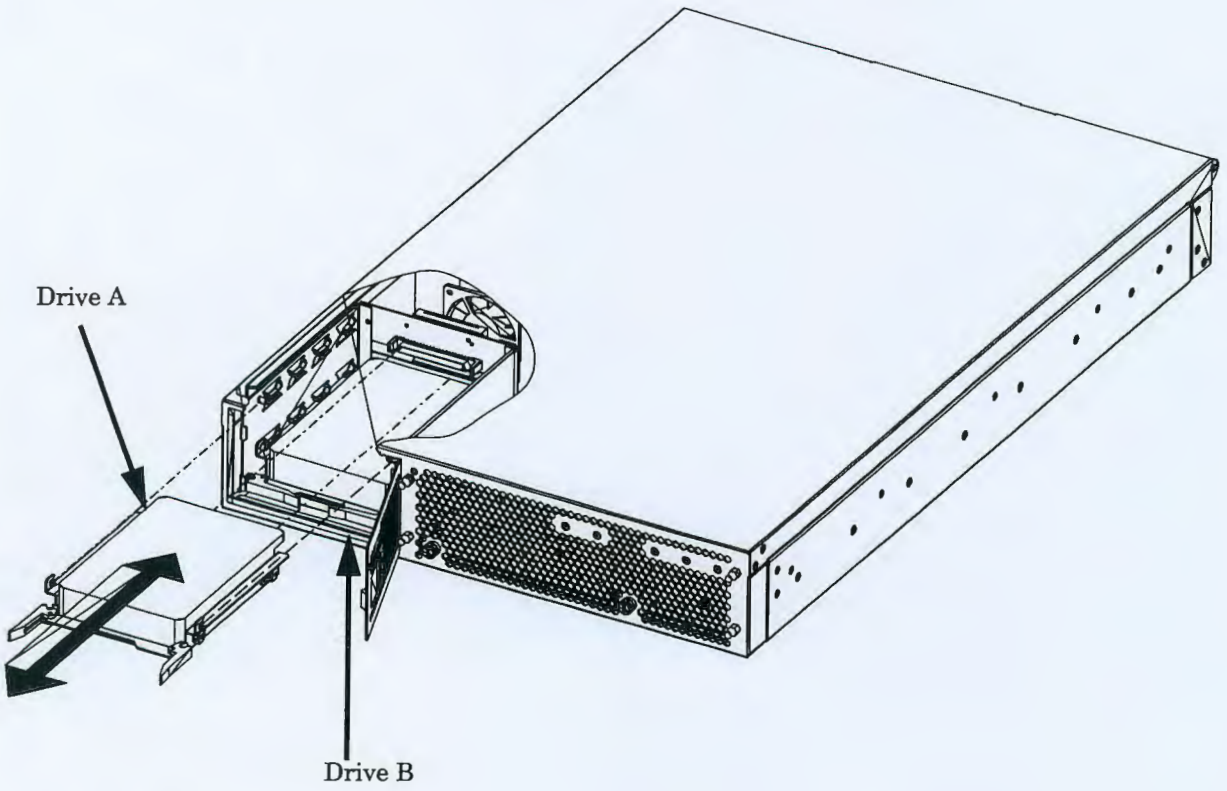
Notes:

1. Use in slot No. 2 ONLY. Cannot be used in slots 1, 3, or 4.
2. Provides web-based console capability on any PC with a browser. If needed, this card must be ordered with the A500 server. Cannot be ordered standalone. This card is not required if a system console terminal is used. Cannot have both A5858A and System Console (C1099A) on the same order.
3. Use A6150-6002 Graphics card in slot 1 only.
4. e3000 systems only.

Add Disks

rp24xx servers support two internal hard disk drives, drive A and drive B.

The following graphic depicts disk drive locations.



ccrr003

(MPE/iX does not support hotswap). It is not necessary to shutdown the HP-UX operating system or power off the server to install a new disk, but you may shutdown HP-UX and power off the server if you choose. The MPE/iX operating system needs to be shutdown prior to installing a new disk and then rebooted.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 677
Doc.

Adding CPUs and Socket Cleaning

Replacement or installation of a CPU requires that the CPU chip socket be clean and uncontaminated with dirt and dust particles. The CPU chip socket must be cleaned or replaced if you:

- Replace a system board (using the CPUs from the old system board to populate the new system board).
- Add a CPU to the server.
- Remove a CPU for troubleshooting (to be replaced in the same system board).
- Remove a failed CPU and replace it with a new CPU assembly.

Tools Required

To add or replace a CPU, or to clean a system board socket and the surrounding area, you will need the following items:

- CPU socket dust cover (HP p/n A3639-40024)
- Electronic Vacuum Cleaner- ESD safe, EMI/RFI line filter, acceptable models and options are:
  1. 110V Vacuum (HP p/n 1150-5070, comes with US power cord)
  2. 220/240V Vacuum (HP p/n 1150-5071, no power cord, must order item 3 or 4)
  3. European power cord (2 meter (6foot)) (HP p/n 5184-0874)
  4. U.K. power cord (2 meter (6foot)) (HP p/n 5184-0875)
  5. Vacuum filter (0.03 micron) (HP p/n 3150-0785)

A magnifying glass, (at least 3X power) to aid in the inspection of the removed CPU socket.

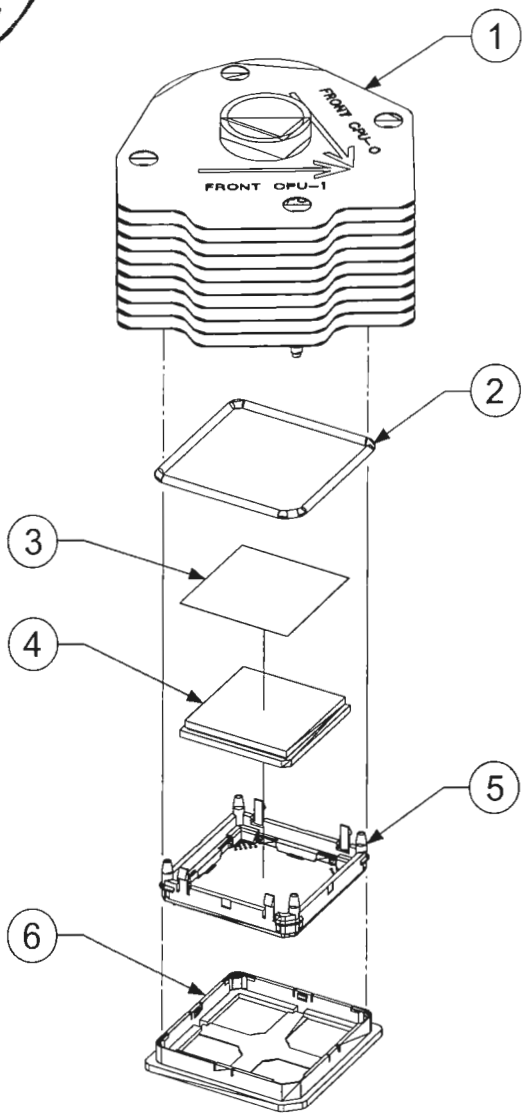
Cleaning Kit Components

The A3639-70001 CPU socket cleaning kit contains the following items.

- EMI O-ring (HP p/n 5183-3542)
- IPA pre-moistened, lint free wipes (HP p/n 5012-1138)
- thermostrate pad (HP p/n A3614-00014)
- CPU chip socket with dust cover (HP p/n 1253-0703)

The following graphic shows an exploded view of the CPU assembly, with the component names.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 678
Doc. 3698



ccrr011

No.	Title
1	Heat Sink
2	EMI O-Ring
3	Thermostrate Pad
4	CPU Chip
5	CPU Chip Socket
6	CPU Chip Socket Dust Cover

CPU Cleaning for System Board Replacement

This section provides information for those situations where CPUs are removed and then replaced onto the same system board or onto a new system board.

1. Carefully vacuum the area surrounding the CPU to be removed and replaced.
2. Remove the CPU assembly.
3. Install the system board socket dust cover (A3639-40024) (item 6) into the empty system board socket.
4. Place the CPU assembly on its side in a clean, ESD safe area.
5. Remove the CPU assembly socket by pressing the four (two on each side) tabs holding the socket to the CPU heat sink base. The CPU chip may come off with the socket or stay attached to the heat sink. (Usually the CPU chip stays in the socket.)
6. Remove the thermostrate pad form the heat sink. It is not necessary to clean the waxy residue left behind on the heat sink and CPU chip.
7. Inspect the system board socket side of the CPU chip for any thermostrate residue. If residue is observed, clean that area with the IPA wipe.

CAUTION Do no attempt to clean the new CPU chip socket buttons.

---

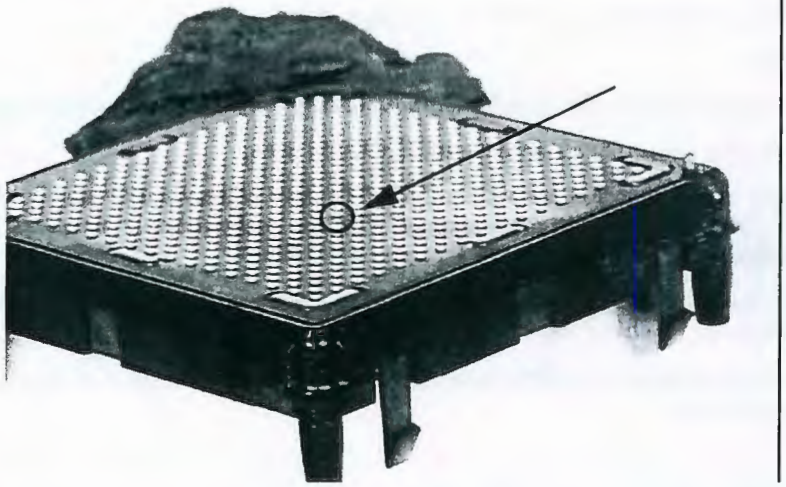
8. Place the CPU chip into the new socket. Match the cut corner of the chip with the angled corner of the socket, and be sure to have the buttons on the chip facing down. The chip should snap into the socket with light downward pressure.
9. Place the O-ring around the outside of the socket's four posts and roll it down against the corner stops.
10. Hold the heat sink assembly upside down (with the bottom up).
11. Place the new thermostrate on the copper base of the heat sink assembly, with the bevelled side down.
12. Lower the CPU chip and socket assembly onto the upside down heat sink. It only snaps in one way.

NOTE Be sure to leave the dust cover on the CPU chip until you are ready to re-install the CPU into the system board.

---

13. Remove the system board socket dust cover installed in step 3 and inspect the old socket for missing or damaged buttons. A hand-held magnifying glass is helpful. Tilt the socket at an angle. Missing buttons will show up as an irregularity in the pattern of contacts. Refer to the photograph below for an example of a socket with a missing button. If missing buttons are observed, take special care in the next step.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 679
3698
Doc.



14. Inspect the CPU socket on the system board for broken buttons or other debris. Note that it is normal for a certain amount of residue to be left behind when removing the CPU assembly. If broken buttons are observed, remove them carefully with the IPA lint free wipe. Take care to contain the debris and completely remove them from the system board socket.
15. Vacuum the system board socket site, being careful not to introduce contaminates in the process.
16. Carefully clean the system board socket with the IPA lint free wipe.
17. Install the CPU assembly into the appropriate CPU socket on the system board.

Installing the CPU

Install CPUs according to the procedure listed below:

Step 1. Carefully align the CPU notches with the socket notches and set the CPU in place.

Step 2. Tighten the four captive T-15 mounting screws that hold the CPU in place.

NOTE Tighten the four CPU mounting screws a little at a time, in a cross pattern (1, 3, 2, 4), until they are all tight.

The following picture shows both CPUs installed in a server.

System Console Configuration

The following describes the steps required to configure the HP C1099A or 700/96 terminal for VT-100 mode for operation with an rp24xx server.

C1099A VT-100 Mode Configuration.

The following procedure outlines the steps to configure the C1099A terminal for VT-100 operation.

To access the Setup menu in HPTerm emulation:

1. Press the **F10** key to display the terminal local function labels, then Press **F8** (*config keys*).

   You are now in the *Quick* (**F1**) menu.
2. Select the VT100 emulation by using the space bar to navigate through the available options.
3. Press the **ESC** key to save selected setup parameters and to exit the *Setup* menu.
4. Press the **Y** key when the blinking prompt

   `Save all? (Y/N)`

   appears in the upper right corner of the menu to save the settings in non-volatile memory.

NOTE If you enter **N** when the

`Save all? (Y/N)`

prompt appears, the changes will take effect, but will be lost if the terminal is reset or powered off.

HP700 VT-100 Mode Configuration

The following procedure outlines the steps to configure the HP700 series terminal for VT-100 operation.

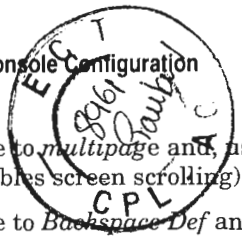
NOTE You may use either the arrow keys or the tab key to move between the setting options on the screen.

Be sure to save any configuration changes you make before proceeding to a new menu.

---

1. Press **[User System]** key.
2. Press **[config keys]** function key. **[f8]**
3. Press **[terminal config]** function key. **[f5]**
4. Move to *Terminal ID* and enter "vt100".
5. Move to *TermMode* and, using the **[Prev]** and **[Next]** keys, select "EM100".
6. Save the configuration. **[f1]**
7. Press the **[config keys]** function key. **[f8]**
8. Press the **[ansi config]** function key. **[f6]**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 681
Doc. 3698



9. Move to *multipage* and, using the **[Prev]** and **[Next]** keys, select "yes". (Enables screen scrolling).
10. Move to *Backspace Def* and, using the **[Prev]** and **[Next]** keys, select "Backspace/Del".
11. Move to *EM100 ID* and, using the **[Prev]** and **[Next]** keys, select "EM100".
12. Save the configuration.**[f1]**

LAN Console

This section describes how to configure a notebook PC as a console via a LAN cable connection. This process uses a terminal emulator software package set to emulate a VT100 terminal.

NOTE The rp24xx server must first be configured via an HP700 system console before accessing it from a PC or UNIX system.

1. Connect a cable between the notebook PC network adapter and the 10BaseT LAN Console port on the rear of the rp24xx server.
2. Launch the terminal emulator software and set emulation to VT100.
3. Connect to the rp24xx server Guardian Service Processor (GSP) by entering its IP address and press **<ENTER>** or **<RETURN>**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
682
Fls. Nº
Doc. 3698

Secure Web Console I/O Card Replacement

The Secure Web Console (SWC) is installed in the rp24xx system as a PCI Card. This option must be included in the initial order of the rp24xx server where it will be installed at the factory during the assembly process. While not available for installation after receipt of the server, it is customer-replaceable if the factory-installed card fails during operation.

Secure Web Console Features

- **Low-level Commands** - A remote operator can exercise powerful, low-level, HP-UX and MPE/ix commands and functions.
- **Remote Server Management** - Provides secure access to the RS-232 low-level console serial port, on supported servers, via the Internet/Intranet.
- **One Person, One Console, Several Servers** - Using a browser, an operator, from a single location, can manage multiple servers, *regardless of where they are located*.
- **Simultaneous Multiple Operator Access** - Up to four operators, *in different locations,* can share the same remote server console at the same time.
- **Security** - Built-in security includes password encryption, scrambled transmission of data, and secure Java download protection.
- **Mirrored Access** - Up to four operators can simultaneously share the remote console screen and keyboard.
- **Universal Browser-based** - Supports both Netscape© v.3.0+ and Microsoft© Internet Explorer v.3.0+ Web browsers.
- **Efficient Server Access** - Operator can *bookmark* servers for multiple server lookup.
- **Upgradable** - HP Secure Web Console firmware is upgradable over the network, making it easy to add new versions and functionality.
- **Internet Standards Compliant** - Supports HTTP, FTP, TFTP, and other key Internet standards.

Secure Web Console PCI Card Replacement

The PCI card version of the SWC is a standard half-card PCI form factor. It is connected to the server by an internal bus connection in lieu of an external RS-232 connection and to the LAN by a twisted-pair cable and an RJ-45 modular plug connection. Refer to the *PCI Card Replacement* instructions for replacement procedures.

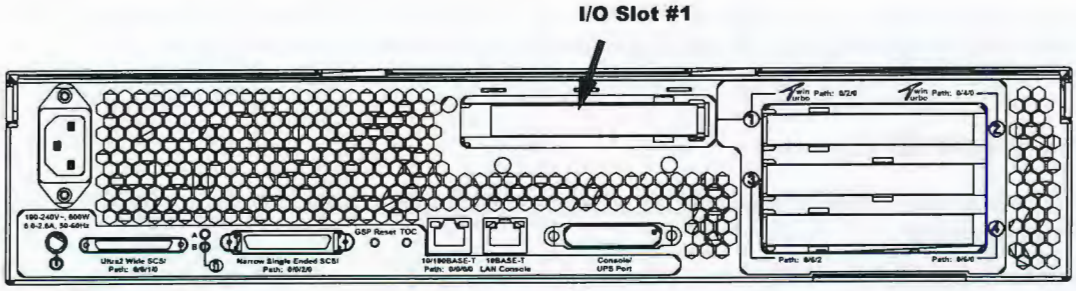
Replacing a SWC card is straightforward. However, proper configuration of the SWC card IP address, plus the complexity of the network, can present problems unless you are properly prepared before hand. It is therefore highly recommended that you:

- *Read and ensure you understand the entire installation and configuration procedure* (Hardware and software) before starting.
- *Acquire all required network information* from the system administrator before starting the installation. (IP addresses, user and administrator names, passwords, etc.).

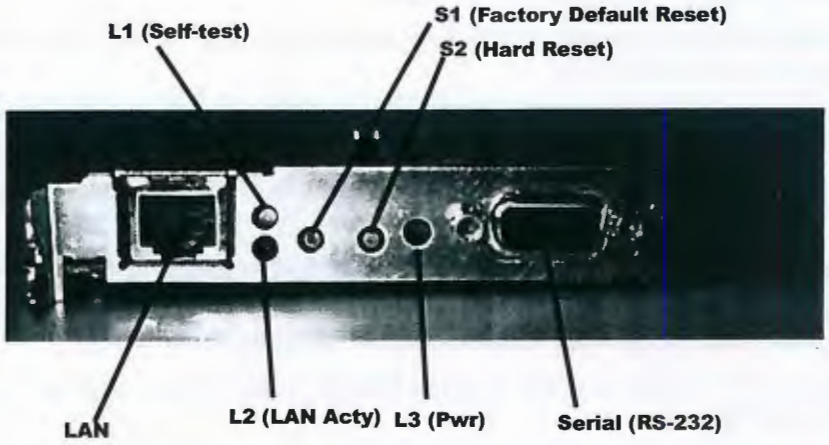
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 683
3698
Doc.

Secure Web Console PCI Card Introduction.

Since the SWC card is half-card size, it will normally be installed on the server rear bulkhead in I/O slot #1 as shown below:



A picture of the SWC card I/O interface connector is included to show location and identity of LEDs, buttons, and ports:



Title	Description
LAN Port	Plug-in for Local Area Network (LAN) connector.
L1 (Self-test)	Lights when self-test is performed.
L2 LAN Activity	When lit, indicates activity between LAN and the SWC card.
L3 Power	When lit, indicates power to the SWC card.
S1 Factory Default Reset	Only effective when pressed simultaneously with S2.
S2 Hard Reset	Momentarily cuts power to the SWC.
Serial Port (RS-232)	Plug-in for RS-232 connector.

NOTE If you press and hold the S2 (Hard Reset) switch, press the S1 (Factory Default Reset) switch, then release S2 while continuing to hold S1, the SWC card will reset to factory specifications.

Pre-Installation Considerations

The following paragraphs provide an outline of the pre-installation items you should address before starting SWC card replacement.

- Obtain an IP address to be assigned to the SWC card.
- Obtain the subnet mask to be assigned to the SWC card.
- Obtain the gateway address for the SWC card. If a gateway address is unavailable use the SWC card's IP address.
- Know the name of the system to be administered by the SWC card.
- Have internet access available to access the on-line installation and configuration procedures, and the troubleshooting tools.
- Ensure that your browser is on the Supported Browsers list
- Configure your Web Browser software options as follows:

  — ***For Microsoft Internet Explorer©:***
  • Turn off the JIT Compiler — (Deselect the **[Java JIT Compiler Enabled]** preferences box).

  — • Disable Proxies (Until final IP address is assigned) or add the 192.0.0.192 to the proxies list.

  — ***For Netscape Communicator©:***
  • Disable Proxies (Until final IP address is assigned) or add the 192.0.0.192 to the proxies list.

NOTE How these configuration settings are made varies with browsers and versions. For specific instructions on how to set these options, check the documentation specific to your browser.

Installing Multiple Secure Web Consoles.

All network devices require unique IP addresses to operate correctly. All SWC cards ship from the factory with the same default IP address: 192.0.0.192.

If another device on the network is using the same address (e.g. 192.0.0.192) the results of the installation will be *unpredictable.*

Dynamic Host Configuration Protocol (DHCP) and the Secure Web Console.

Every computer on the internet or intranet has a unique TCP/IP number/address. Traditionally, TCP/IP numbers are assigned by hand. DHCP is a protocol that allows the assignment of IP addresses *on-the-fly,* for a single session use, from a pool of numbers that the DHCP server controls. Typically, you can use DHCP to preconfigure SWCS permanent network parameters. For more information, go to the SWC DHCP web page at: http://www.docs.hp.com/hpux/onlinedocs/hw/swc/install/00096I/index.htm

NOTE Only DHCP on HP-UX is supported.

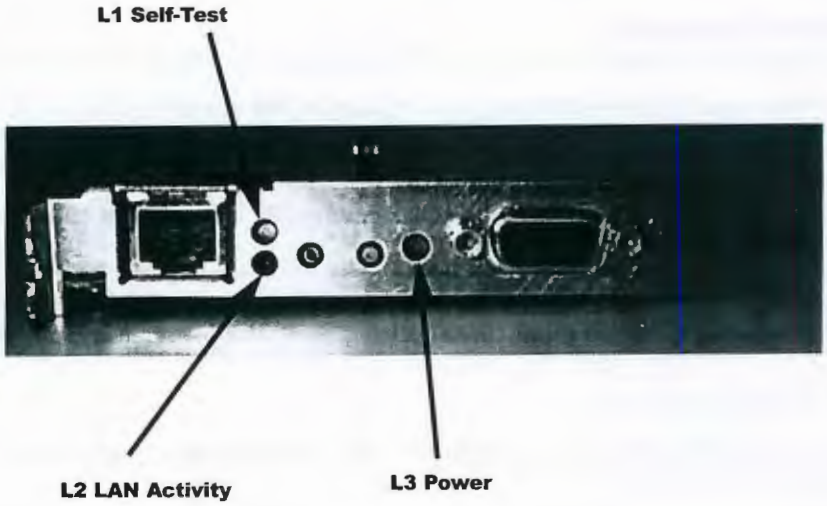
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Initial Cable Connections

To make the cable connections, proceed as follows:

Step 1. Connect the SWC card to the Intranet/internet (LAN).

Step 2. Observe the LEDs on the SWC card rear bulkhead connector.



LED Indications

Solid Amber	Self-Test in progress
Amber Off	Self-Test completed
Amber Stays On	Self-Test Failed
Flashing Green (LAN)	Network Activity
Solid Green (Power)	Power on

CAUTION For system security, initial configuration must be completed *before* making the serial connection between the SWC card and the server's console port.

Failure to follow this precaution can result in root level access being available to any level of SWC user.

Step 3. Connect the server's console to the SWC card via the RS 232 Serial port.

RS 232 Serial Port

Step 4. Perform Initial Configuration of the SWC card.

a. Ensure that no other devices (printers, etc.) are connected *on the same local subnet* by disconnecting the LAN cable from the SWC and using the *Ping* command as follows:

```
C:\ ping 192.0.0.192
```

It will time out.

b. At a command line prompt, enter the following:

```
C:\route add 192.0.0.192 xx.xx.xx.xx.xx
```

Where *xx.xx.xx.xx.xx* is the IP address of your PC or Unix workstation.

c. Reconnect the LAN cable to the SWC card and use a PC or Unix Workstation and a web browser. Verify that you can access the SWC at its default IP address using the *Ping* command as follows:

```
C:\ping 192.0.0.192
```

It will indicate connection with the SWC card at IP 192.0.0.192

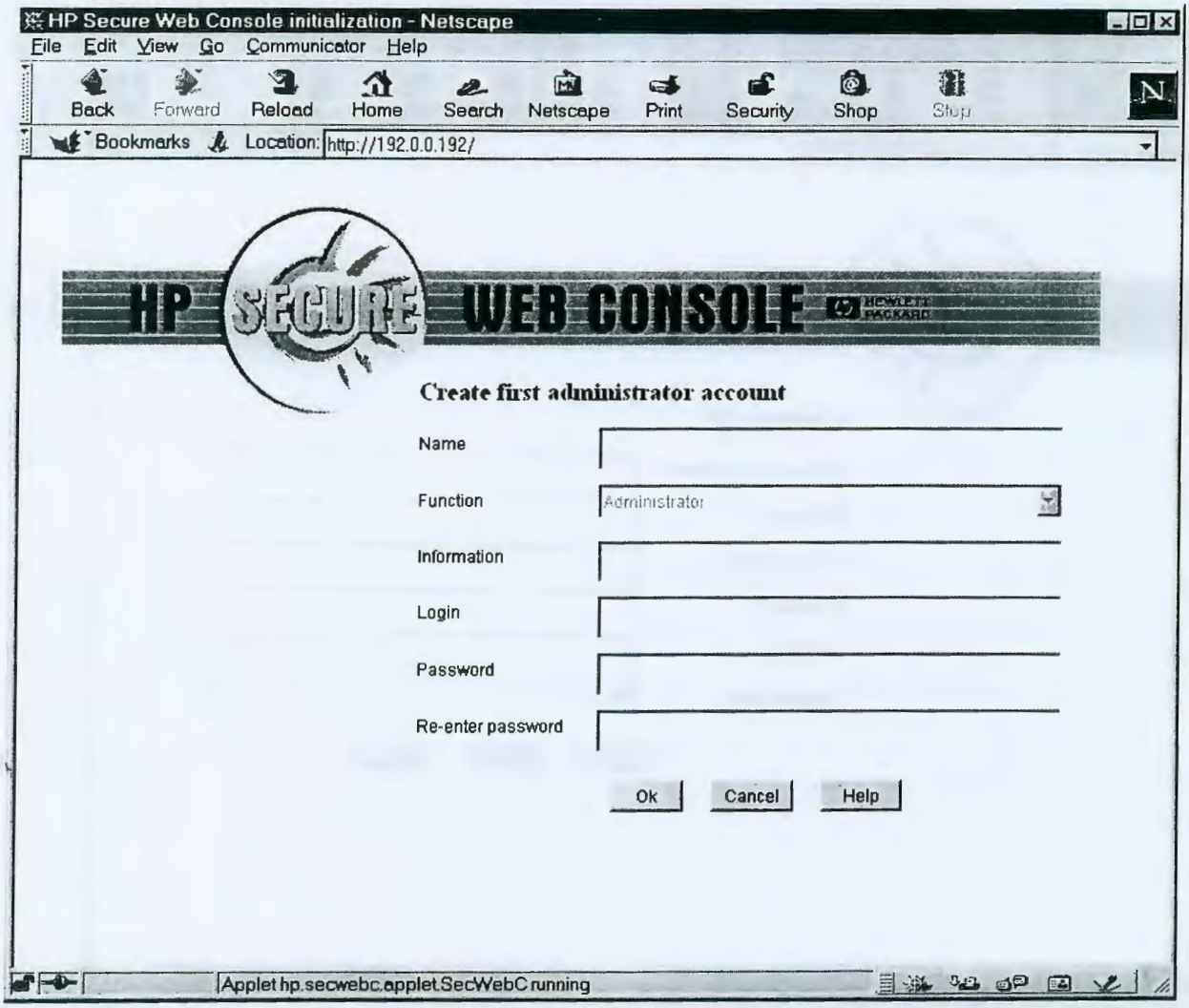
Step 5. Create the first SWC administrator account.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0853
Fls. Nº
Doc. 3698

NOTE The SWC requires creation of the first administrator account before proceeding further.

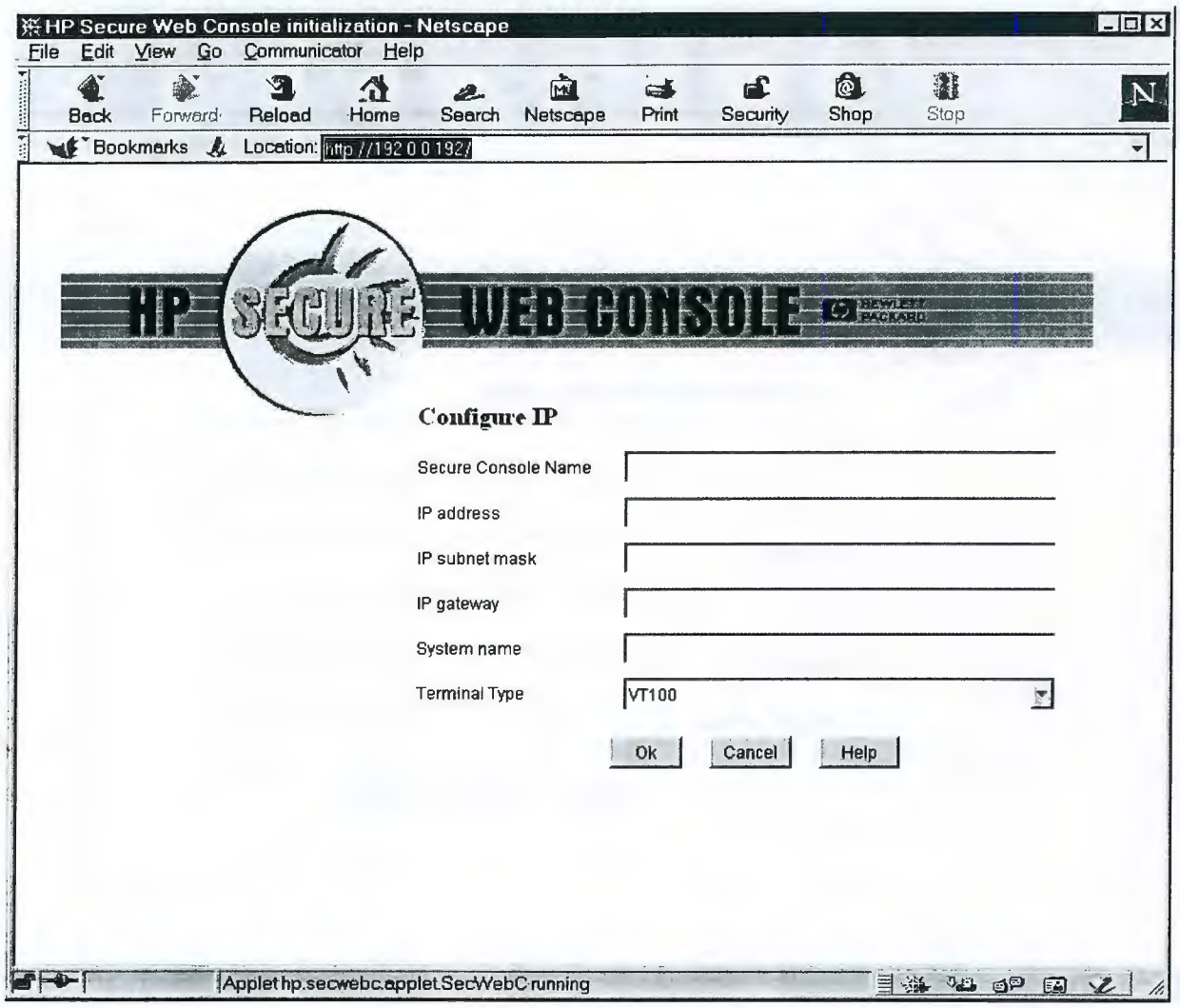
a. Using a web browser, access the SWC at the default IP address (192.0.0.192).

b. To create the first SWC administrator account, fill in the prompts shown in the following illustration:



RQS nº 03/2008 - CN
CPMI - CORREIOS
Fls. Nº 686
Doc.

c. To configure the network parameters for the SWC, fill in the prompts shown in the following illustration:



d. When all necessary data is entered, click on [OK] to reboot the SWC.

Step 6. Using a web browser, connect to the SWC card, using:

- the newly assigned IP address, and
- the newly created administrator log-in and password.

NOTE It may take as much as 45 seconds to gain initial access to the SWC card.

Step 7. Connect the serial cable between the SWC card and the server's console port.

Table 7-1 (Continued)

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**CRU**	**Action to Take**
8 - I/O	6 - Disk	N/A	Various Values	Disk Subsystem	Use BCH commands and ODE diagnostics to check disk subsystem.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 687
Doc. 3698

E C T
CPL - AC

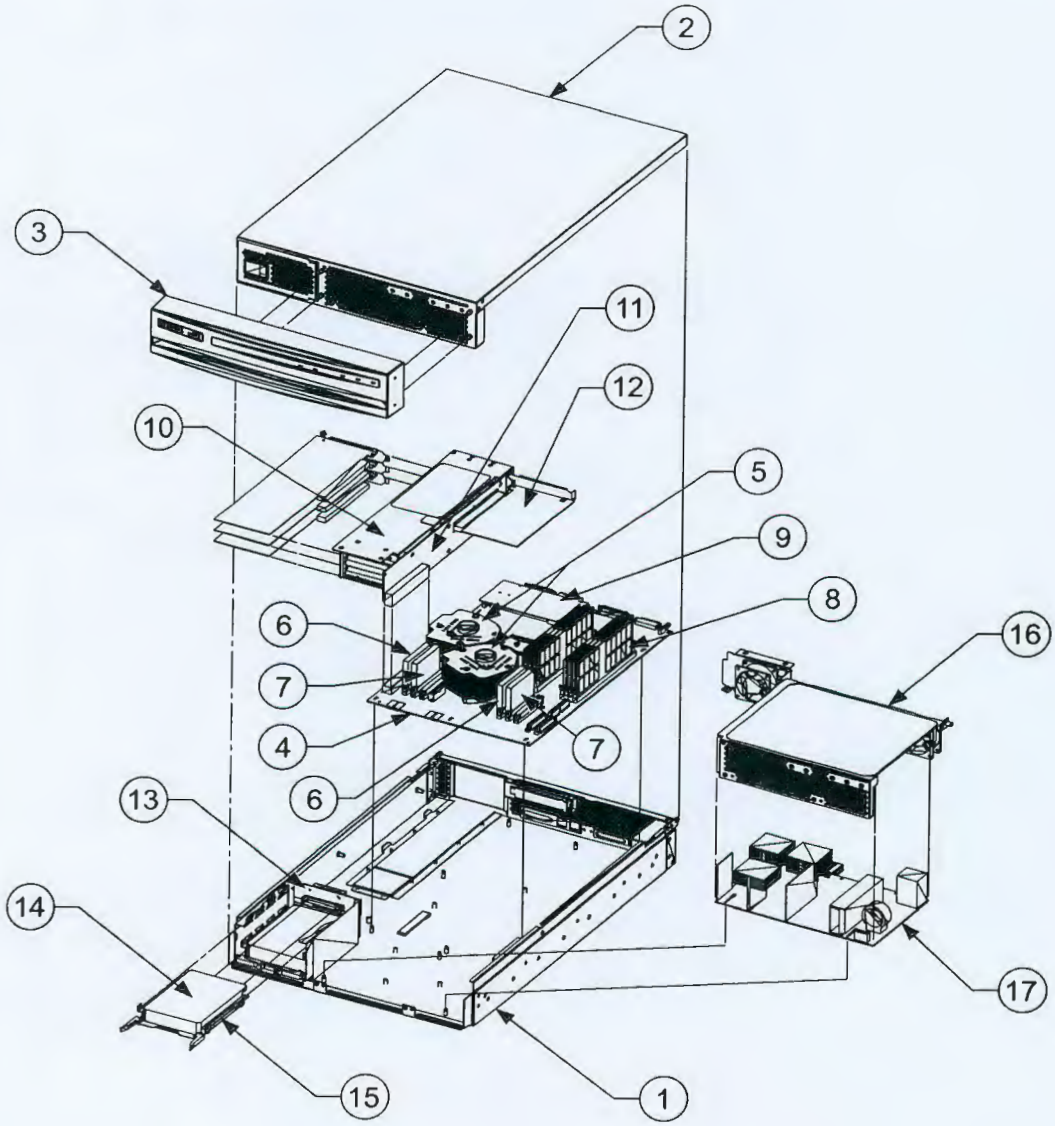
9 Server Component Removal and Replacement Procedures

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 688
3698
Doc.

ECT 8939 fls. 2 CPL - AC

Customer Replaceable Unit (CRU) Physical Location

This section contains views of the rp24xx server. The locator numbers in the diagrams correspond to the numbers in the CRU Part Number section.



ccrr009

NOTE Components numbered 1, 4, 5, 13, 16. and 17 are not customer replaceable and do not appear in the Customer Replaceable Unit (CRU) Part Numbers section. They are included in this illustration for continuity, only.

ECT 8939 fls. 2 CPL - AC
IBOSI nº 08/2005 - CN
CPMI - CORREIOS
Fls. Nº 689
Doc. 3690

E C T
8934
Paula
CPL - AC

Customer Replaceable Unit (CRU) Part Numbers

The following tables list all Customer Replaceable Units (CRUs) for the rp24xx server. CRUs may be removed or replaced by either the customer or by qualified HP field engineering personnel. Table 1 lists both new and exchange part numbers. Table 2 lists only the new part numbers for non-exchange CRUs.

Exchange CRUs

Product #	New Part #	Exch. Part #	Description	Loc. #
A6114A	A6114-60001	A6114-69006	2048 MB Memory DIMM	8
A5841A	A5841-60001	A5841-69001	1024 MB Memory DIMM	
A5840A	A5840-60001	A5840-69001	512 MB Memory DIMM	
A5572A	A5572-60002	A5572-69002	128 MB Memory DIMM	
A5505A	A5505-60001	A5505-69001	9 GB Disk Drive	14
A5531A	A5531-60001	A5531-69001	18 GB Disk Drive	
A6089A	A6089-67001	A6145-69001	36 GB Disk Drive	
A5570A	A5570-60002	A5570-69002	Guardian Service Processor	9

Non Exchange CRUs

Part #	Description	Loc #
A5570-60003	PCI I/O Backplane	11
A5570-60005	Secure Web Console PCA	12
A5570-00002	Disk Carrier	15
0950-3821	DC-DC Converter - Master	6
0950-3822	DC-DC Converter - Slave	7
A5570-62003	I/O Card Cage Chassis	10
A5570-62006	Plastic Front Bezel	3
A5570-67007	Chassis Top Cover	2
A5570-84001	rp2450 Name Plate	N/A
A5191-63001	Console-Remote-GSP Cable	N/A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 690
Doc. 3698

Front Bezel Removal

The rp24xx server does not have to be turned off to remove the bezel.

WARNING **Do not attempt to lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency. Failure to heed this warning may result in personal injury and/or permanent damage to the server.**

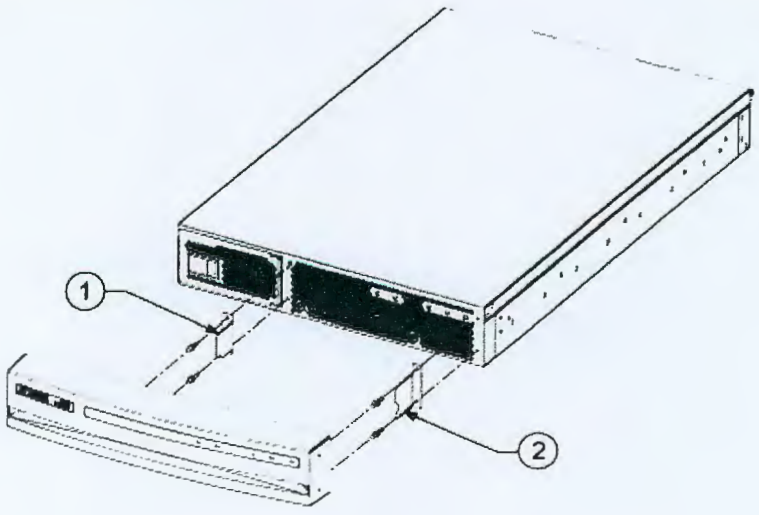
Removing the bezel provides access to the following:

- HotPlug Disk Drive access door.
- Two knurled thumbscrews that secure the server cover.

To remove the bezel, grasp the bezel at the sides and pull straight out until it is free of the bezel retainers and ball-posts on the server.

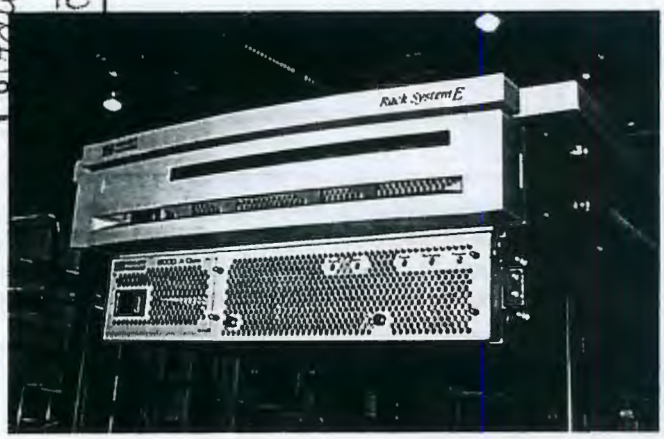
CAUTION Pull the bezel straight out. Do not twist or wiggle from side-to-side any more than necessary to keep from damaging the bezel sockets.

The following illustration shows a server and bezel with the bezel retainers and ball posts in an exploded view.



The following picture shows one server with the front bezel attached and one server without.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 691
Doc.


Rack System E

Front Bezel Replacement

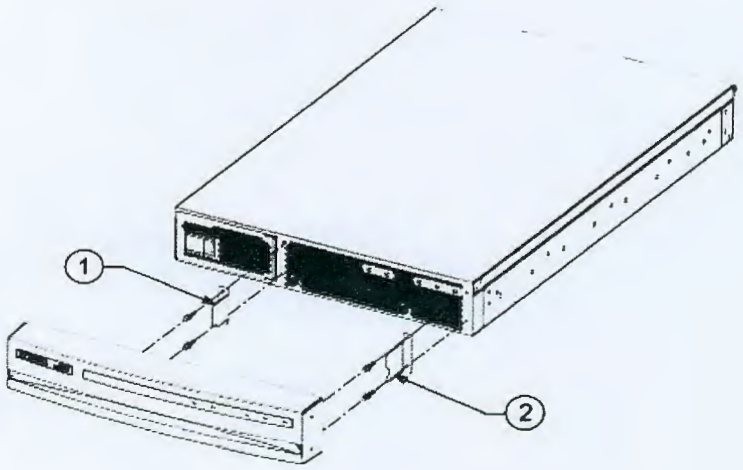
The rp24xx server does not have to be turned off to replace the bezel.

WARNING **Do not lift or carry the server by the bezel. The bezel is made of plastic and is attached to the server chassis by two bezel retainers and four ball-posts. It will only support the weight of the server chassis in an emergency.**
Failure to heed this warning may result in personal injury and/or permanent damage to the server.

To replace the bezel, grasp the bezel at the sides and align the bezel sockets with the bezel retainers and ball-posts on the server and push straight in. The bezel will lock into place.

CAUTION During replacement, do not twist or wiggle the bezel from side-to-side any more than necessary to keep from damaging the bezel socket.

The following illustration shows a server and bezel with the bezel retainers and ball posts in an exploded view.



As you are facing the front of the server, item 1 is the left bezel retainer with two ball posts, and item 2 is the right bezel retainer with two ball posts.

CAUTION Left and right bezel retainers are NOT interchangeable.

The following picture shows one server with the front bezel attached and one server without.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 699
Doc.

Server Cover Removal

The cover that protects rp24xx server components is secured by two thumbscrews and, when released, slides forward for removal.

To remove the cover, perform the following procedures:

Step 1. Remove the front bezel.

WARNING **There is a safety interlock between the front of the server cover and the Power Supply. When the cover is taken off, power is automatically removed from the server if power cords were not detached previously.**

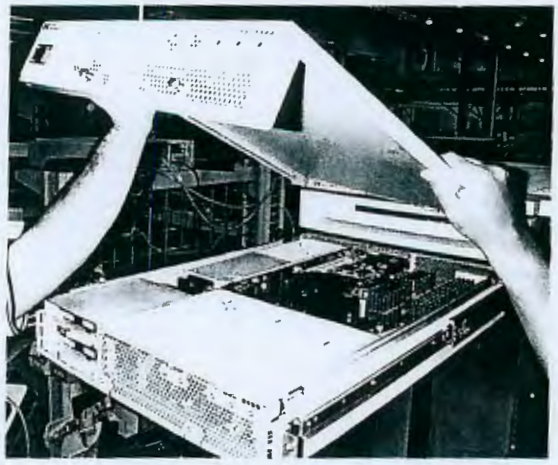
DO NOT attempt to defeat this interlock. Doing so will expose you to high levels of electrical amperage that can cause serious injury or death.

Step 2. Unfasten the two captive knurled thumbscrews located near the bottom edge of the front of the server cover.

Step 3. Grasp the thumb screws and pull the cover toward you. Slide the cover approximately 2.5 MM (1 in.) then lift the cover front to clear the notches on each side of the server. Set the cover aside.

CAUTION The server weighs approximately 23 kg (50 lbs). Take necessary precautions to prevent muscle strain when lifting and carrying the server.

The following graphic shows the server cover suspended over the server.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 693
3698
Doc.

CPL - A
8930
Paula

Server Cover Replacement

The cover that protects rp24xx server components must be raised in front and positioned on top of the side chassis panels then lowered and slid into the back chassis panel. The cover is secured by two thumbscrews attached to the front chassis panel.

To replace the cover, perform the following procedures:

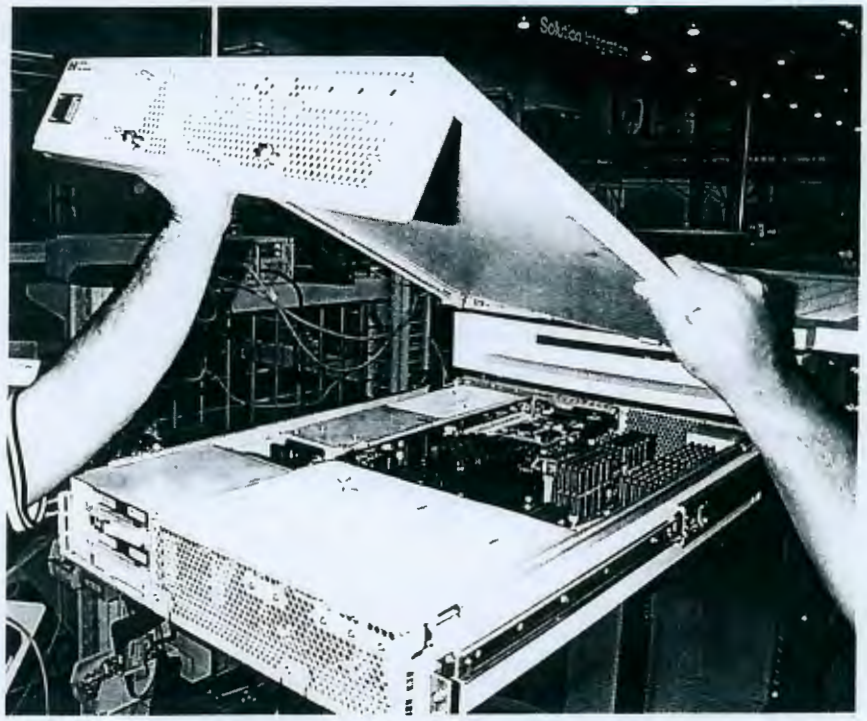
Step 1. Tilt the cover front up slightly and position it on top of the chassis side panels approximately 2.5 MM (1 in.) from the rear of the server chassis.

Step 2. Lower and slide the cover back over the notches on each side of the front of the server and seat it against the rear chassis panel.

Step 3. Fasten the two captive knurled thumbscrews located near the bottom edge of the front of the server cover.

CAUTION The server weighs approximately 23 kg (50 lbs). Take necessary precautions to prevent muscle strain when lifting and carrying the server.

The following graphic shows the server cover suspended over the server.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 691
3098
Doc.

ECT CPL - AC

HotPlug Disk Drive Removal (HPUX Systems Only)

The disk drives (up to two) are located at the front left side of the server (as you are facing it). When proper software and hardware procedures are followed, these disk drives can be removed and replaced while the server is running.

NOTE MPE/iX does not support hotswap. Do not use these procedures on HP e3000 servers.

The procedures in this section are in two parts, a software HotPlug procedure to prepare the drive for removal and the hardware procedures for physically removing the device from the server.

Before starting these procedures, you must have an up-to-date configuration backup file. Configuration backup is performed by default each time an LVM command changes the LVM configuration. The default backup file path is:

```
/etc/lvmconf/base_vg_name.conf
```

The replacement disk drive must be the same product ID as the disk drive that is being replaced.

NOTE HP often uses different manufacturers for disks that have the same product number. The HotPlug manual procedure will not update the disk drivers internal information to that of the replaced disk drive.

The replacement disk drive will have the same capacity and blocksize as the defective disk because they have the same product number. The only field that can be incorrect is the string specifying the vendor's name. This will not affect the behavior of the LVM. If you desire to update the manufacturer's name, the disks volume group must be deactivated and reactivated.

HotPlug Software Procedure

NOTE The HotPlug software procedures for Disk Drive removal/replacement described below are for a mirrored boot disk configuration only. If your configuration differs from this, these procedures may not be valid. Consult your System Administrator or contact the HP Response Center for assistance.

Perform these software procedural steps to replace a HotPlug disk drive device:

Step 1. Determine whether or not the LVM found the physical volume to be defective when the volume group was activated.

If the volume was defective when the volume group was activated, *vgchange* would have generated the following message to the console:

```
WARNING

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
VOLUME "/DEV/DSK/cXtXdX"

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 695
Doc 3698

```
VOLUME "/DEV/DSK/cXtXdX"

THE PATH OF THE PHYSICAL VOLUME REFERS TO A DEVICE THAT DOES NOT
EXIST, OR IS NOT CONFIGURED INTO THE KERNAL.
```

If you are unsure of the status of the *vgchange*, you may check if this occurred by typing the *vgdisplay* command: *vgdisplay <VG name>*. For example:

```
# vgdisplay /dev/vg00
```

If you see these messages, the disk was defective at the time the volume group was activated. Remove the bad disk as described in the *HotPlug Hardware Procedure* section, then follow the instructions in *Disk Drive Replacement* for replacing the disk and perform the Hot Swap Procedure for Unattached Physical Volumes described there. Otherwise, your disk drive became defective after the *vgchange* and you must continue with step 2 of this section.

Step 2. Display the names of all the logical volumes on this volume group using the *vgdisplay* command. For example:

```
#vgdisplay /dev/vg00
```

Step 3. Determine which logical volumes have mirrors by using the *lvdisplay* command. For example:

```
#lvdisplay /dev/vg00/lvol# | grep -ie "LV Name" -e
"Mirror"
```

Step 4. Determine the *pvkey* for the mirrored logical volume, again using the *lvdisplay* command with the *-k* option. Compare the output to the *lvdisplay* command with the *-v* option to determine the device file to *pvkey* mapping. For example,

```
# lvdisplay -v -k /dev/vg00/lvol1

--- Logical volumes ---
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
LV Permission               read/write
LV Status                 available/syncd          Mirror copies
1         Consistency Recovery      MWC              Schedule
parallel    LV Size (Mbytes)          256            Current LE
64       Allocated PE             128        Stripes                  0
Stripe Size (Kbytes)      0              Bad block               off
Allocation               strict/contiguous       IO Timeout (Seconds)
default           --- Distribution of logical volume ---PV Name           LE
on PV  PE on PV  /dev/dsk/c1t6d0   64      64      /dev/dsk/c2t6d0   64
64

--- Logical extents ---LE        PV1        PE1   Status 1 PV2          PE2
Status 2 00000     0       00000 current  1          00000 current  00001
0        00001 current  1           00001 current  00002     0        00002
current  1          00002 current  00003     0       00003 current  1
00003 current  00004     0        00004 current  1           00004 current
00005     0       00005 current  1          00005 current  00006     0
00006 current  1           00006 current  00007     0        00007 current
1            00007 current  00008     0         00008 current  1
00008 current  (etc.)
# lvdisplay -v /dev/vg00/lvol1--- Logical volumes ---LV Name
/dev/vg00/lvol1VG Name                     /dev/vg00LV Permission
```

```
read/write     LV Status                    available/synced      Mirror
copies              1          Consistency Recovery          MWC
Schedule                    parallel     LV Size (Mbytes)            256
Current LE                    64         Allocated PE                128
Stripes                     0       Stripe Size (Kbytes)        0
Bad block                     off          Allocation
strict/contiguous           IO Timeout (Seconds)        default             ---
Distribution of logical volume ---PV Name             LE on PV  PE on PV
/dev/dsk/c1t6d0    64         64         /dev/dsk/c2t6d0    64         64
--- Logical extents ---LE    PV1                 PE1   Status 1 PV2
PE2    Status 2 00000 /dev/dsk/c1t6d0     00000 current  /dev/dsk/c2t6d0
00000 current  00001 /dev/dsk/c1t6d0     00001 current  /dev/dsk/c2t6d0
00001 current  00002 /dev/dsk/c1t6d0     00002 current  /dev/dsk/c2t6d0
00002 current  00003 /dev/dsk/c1t6d0     00003 current  /dev/dsk/c2t6d0
00003 current  00004 /dev/dsk/c1t6d0     00004 current  /dev/dsk/c2t6d0
00004 current  00005 /dev/dsk/c1t6d0     00005 current  /dev/dsk/c2t6d0
00005 current  00006 /dev/dsk/c1t6d0     00006 current  /dev/dsk/c2t6d0
00006 current  00007 /dev/dsk/c1t6d0     00007 current  /dev/dsk/c2t6d0
00007 current  00008 /dev/dsk/c1t6d0     00008 current  /dev/dsk/c2t6d0
00008 current
```

The *pvkey* (0 or 1 in this example) shown in the first command maps to the device file names (/dev/dsk/c1t6d0 or /dev/dsk/c2t6d0) in the second command under columns PV1 and PV2, respectively.

Step 5. Reduce any logical volumes that have mirror copies on the faulty disk drive so that they no longer mirror onto that disk drive (note the *-A n* option):
 # lvreduce -m 0 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>& (for one-way mirroring)
OR
 # lvreduce -m 1 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>& (for two-way mirroring).

For example:
 # lvreduce -m 0 -A n -k /dev/vg00/lvol4 /dev/dsk/c2t4d0 1&

The following message will appear:

```
Logical volume /dev/vg00/lvol4 has been successfully reduced.
lvlnboot: Logical Volume has no extents
```

It is important to include the ampersand (&) at the end of the command line. This *lvreduce* process will hang, and you will need terminal control to kill the command. Once the "successfully reduced" message has been generated, manually kill the process, using the kill -9 command.

a. Use the *ps* command to find the PID for the *lvreduce* process.

```
# ps -ef | grep lvreduce
```

b. Stop the process. (This may take several minutes before the process finally ends.

```
# kill -9 <PID>
```

Step 6. Repeat steps 4 and 5 for all logical volumes.

Step 7. With all logical volumes reduced, now reduce the volume group using the *vgreduce* command. For example:

```
# vgreduce /dev/vg00 /dev/dsk/c2t6d0
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 606
3698
Doc.

The *vgreduce* process may take a long time to complete. Do NOT kill this process.

Step 8. Update the disk BDRA using the *lvlnboot* command.

```
# lvlnboot -R
```

HotPlug Hardware Procedures

CAUTION (MPE/iX does not support hotswap). Disk Drives can be removed or installed with the server still powered on. This is referred to as a "manual HotPlug". However, DO NOT remove a HotPlug disk drive until all prior software procedures have been completed. The MPE/iX operating system needs to be shut down prior to installing a new disk and then rebooting.

To remove a bad disk drive from the server, perform the following steps:

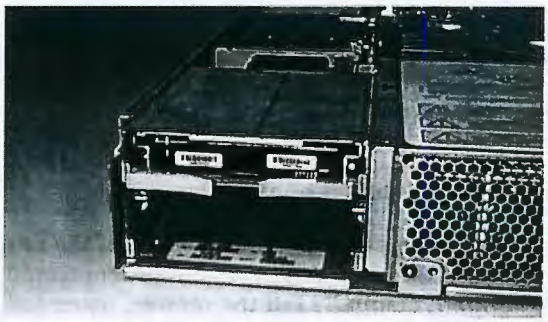
Step 1. Remove the front bezel.

Step 2. On the left side of the front of the server you will see a door with a spring-loaded latch holding it shut. Open the door to expose the disk drive slots.

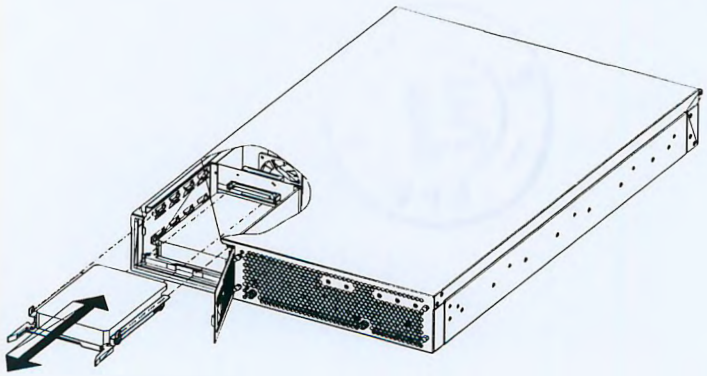
Step 3. Perform the following steps in the order shown:

1. Pull out on the extraction levers on each side of the selected disk drive to unlock it.
2. Pull gently on the levers to pull the disk drive partially out of its slot
3. Wait 10 seconds for the drive to spin down.
4. Grasp the disk drive, pull it completely out of its slot, and set it aside.

The following photograph shows a HotPlug disk installed in the disk housing.



The following graphic shows the location of the HotPlug disks.



ccrr003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 697
3698
Doc.

HP-UX HotPlug Disk Drive Replacement

The internal disk drives (two) are located at the front left side of the server (behind the bezel). When proper software and hardware procedures are followed, internal disk drives can be removed and replaced while the server is running.

NOTE MPE/iX does not support hotplug. Do not use these procedures on HP e3000 servers.

The procedures in this section are in two parts: physically replacing the device in the server and performing the HotPlug software procedure.

The replacement disk drive must be the same product ID as the disk drive that is being replaced.

HotPlug Hardware Procedure

Be sure that all the software procedures in the Disk Drive Removal section have been performed prior to starting these steps.

To install a disk drive from the server, perform the following steps:

Step 1. Remove the front bezel.

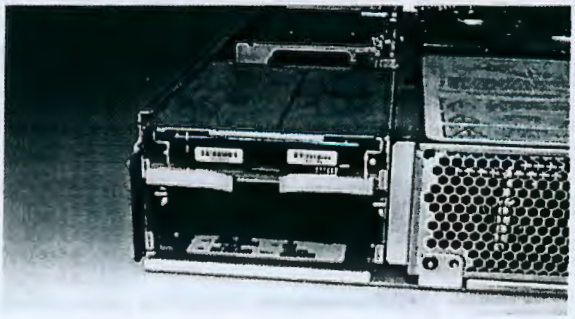
Step 2. On the left side of the front of the server you will see a door with a spring-loaded latch holding it shut. Open the door to expose the disk drive slots.

Step 3. Align the drive and carefully slide it completely into the selected slot with the extraction levers out.

Step 4. Fold the extraction levers in to engage and lock the disk drive in place.

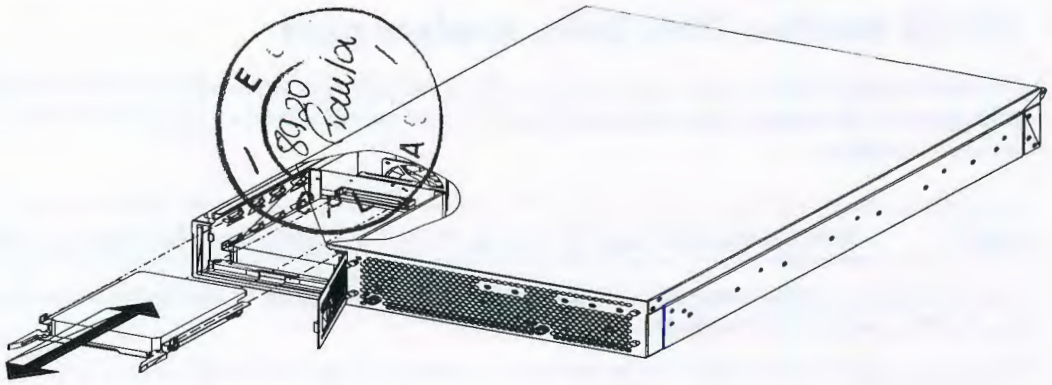
Step 5. Close the door and engage the spring-loaded latch to keep it shut.

The following photograph shows a HotPlug disk installed in the disk housing.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 698
3698
Doc.

The following graphic shows the location of the HotPlug disks.



ccrr003

HP-UX HotPlug Software Procedure

NOTE The HP-UX HotPlug software procedures for Disk Drive removal/replacement described below are for a mirrored boot disk configuration only. If your configuration differs from this, these procedures may not be valid. Consult your System Administrator or contact the HP Response Center for assistance.

HP-UX HotPlug Software Procedure for Attached Physical Volumes

Follow this procedure if the disk that was removed was recognized as an attached physical volume.

NOTE HP often uses different manufacturers for disks having the same product number. The HotPlug manual procedure will not update the disk drivers internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed) and also as a double check that it is a proper replacement and the device files are present. Refer to the above note. For example:

```
# ioscan -fnC disk
```

Step 2. Mirror the root disk:

a. Create the new physical volume using the *pvcreate* command. For example:

```
#pvcreate -B /dev/rdsk/cXtXdX
```

b. Extend the volume group to include the new physical volume using the *vgextend* command. For example:

```
#vgextend /dev/vg00 /dev/dsk/cXtXdX
```

c. Run the *mkboot* command to make the device bootable. For example:

```
#mkboot /dev/rdsk/cXtXdX
```

d. Use the *mkboot* command again to add the HP-UX auto-file-string. For example:

```
#mkboot -a "hpux" /dev/rdsk/cXtXdX
```

e. Run *lvlnboot*. For example:

```
#lvlnboot -R
```

f. *lvextend* a mirror into the replaced disk drive. This may take several minutes because this function copies all the data from the original copy of the data to the mirrored extents. The logical volume(s) are still accessible for users' applications during operation of this command.

```
#lvextend -m 1 <LV name> /dev/dsk/cXtXdX
```

For example:

```
#lvextend -m 1 /dev/vg00/lvol4/dev/dsk/cXtXdX
#lvextend -m 1 /dev/vg00/lvol5/dev/dsk/cXtXdX
```

Repeat this procedure for each logical volume to be mirrored

Step 3. Verify that the mirror is bootable and AUTO file is correct.

```
#lifls -l /dev/rdsk/cXtXdX
#lifcp /dev/rdsk/cXtXdX:AUTO -
```

Step 4. Verify that the mirroring is set up properly.

```
#vgdisplay -v /dev/vg00
#lvdisplay /dev/vg00/lol1 - lvol8
#lvlnboot -v /dev/vg00
```

Both disks should list as "Boot Disk" and both should appear in the *lvol* lists.

At this point, the system is fully functional.

HP-UX HotPlug Procedure for Unattached Physical Volumes

Follow these steps to replace a HotPlug disk drive for unattached physical volumes.

NOTE HP often uses different manufacturers for disks having the same product number. The HotPlug manual procedure will not update the disk drivers internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed) to verify that it is a proper replacement and the device files are present. Refer to the above note. For example:

```
# ioscan -fnC disk
```

Step 2. Restore the LVM configuration/headers onto the replaced disk drive from your backup of the LVM configuration:

```
#vgcfgrestore -n <volume group name> /dev/rdsk/cXtXdX
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 699
Doc. 3698

For example:

```
#vgcfgrestore -n /dev/vg00 /dev/rdsk/c2t4d0
```

Step 3. Attach the new disk drive to the active volume group with the *vgchange* command.

```
# vgchange -A y <volume group name>
```

For example:

```
# vgchange -A y /dev/vg00
```

Step 4. Run the *mkboot* command to make the device bootable. For example:

```
#mkboot /dev/rdsk/cXtXdX
```

Step 5. Use the *mkboot* command again to add the HP-UX auto-file string. For example:

```
#mkboot -a "hpux" /dev/rdsk/cXtXdX
```

Step 6. Run *lvlnboot*:

```
#lvlnboot -R
```

Step 7. Resynchronize the mirrors of the replaced disk drive. This may take several minutes since it has to copy all the data from the original copy of the data to the mirrored extents. The logical volume(s) are still accessible for users' applications during operation of this command.

```
#vgsync <VG name>
```

For example:

```
#vgsync /dev/vg00
```

The system is now functional.

I/O Card Cage Removal

The I/O Card Cage is located at the rear left side of the rp24xx server. To remove the I/O Card Cage, follow the steps listed below:

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

Step 1. On the rear bulkhead, remove cables attached to I/O card slots 2 through 4, located inside the card cage. Remove the cable attached to I/O card slot 1, located outside the card cage.

Step 2. Within the chassis, remove the I/O card from slot 1 on the right side of the I/O Card Cage, attached to the I/O Backplane as follows: If the card in slot 1 is a Secure Web Console card, unplug the 5V power connector from the receptacle on the card.

a. Remove the screw that attaches the I/O card to the rear bulkhead.

NOTE A short-shaft or right-angle Phillips-head screwdriver must be used to remove the screw due to the short distance between the screw head and the right side of the chassis.

b. Pull the I/O Card out of its slot on the I/O Backplane and place it on a clean anti-static surface.

Step 3. Loosen the two captive Phillips-head screws located at the front of the Card Cage.

Step 4. Grasp the flat lever handle on the right side of the Card Cage and pull it up and forward to release the I/O Backplane from the System Board.

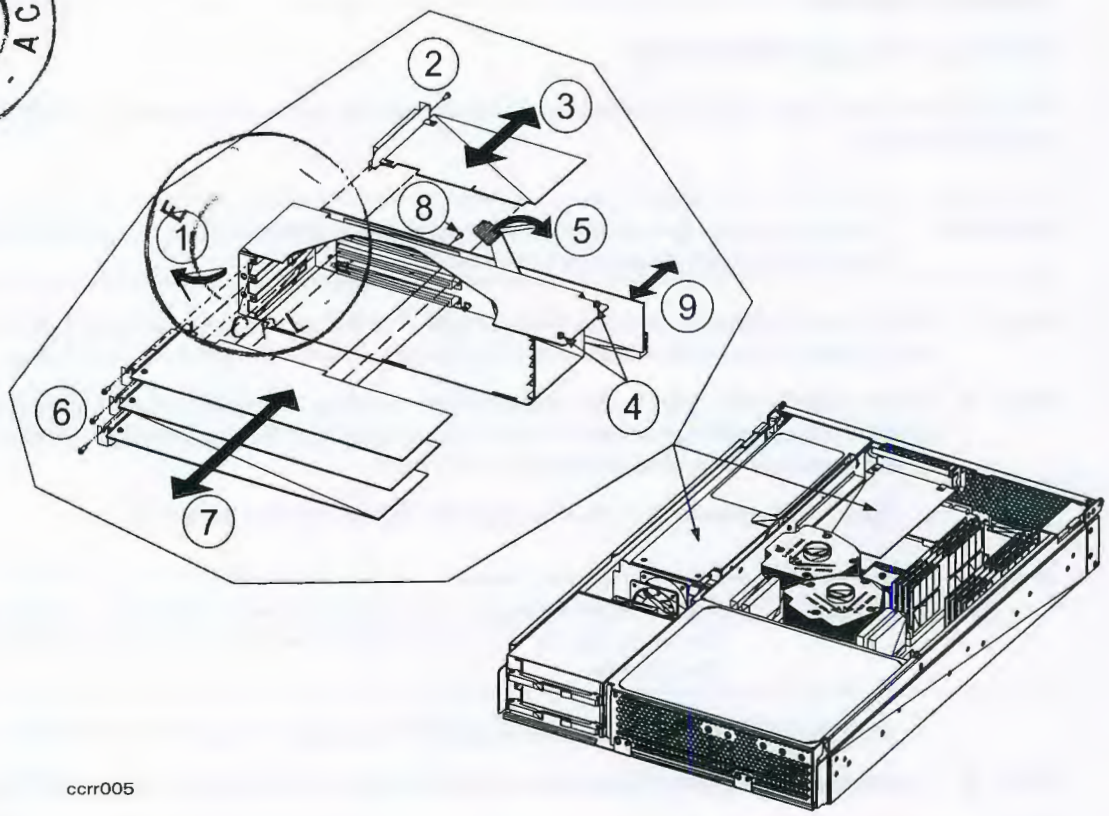
Step 5. Grasp the I/O Card Cage, tilt the front up, and pull it up and out of the chassis.

CAUTION Do not scrape the I/O Backplane against the CPU heat sink when you lift the card cage out of the chassis.

The following photograph shows an empty I/O Card Cage.

The following graphic shows an I/O Card Cage.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 708
3698
Doc.



ccrr005

No.	Title
1	I/O Card Cage
2	I/O Card #1 slot tab
3	I/O Card #1 (short card only)
4	Top front captive screws
5	Flat lever handle
6	I/O Cards #2 through 4 slot tabs
7	I/O Cards #2 through 4 (long or short cards)
8	I/O Backplane retainer screw
9	I/O Backplane

I/O Card Cage Replacement

The I/O Card Cage is located at the rear left side of the rp24xx server. To replace the I/O Card Cage, follow the steps listed below:

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

Step 1. Grasp the I/O Card Cage, tilt the front up, and slide it down and into the chassis.

CAUTION To prevent damage to the I/O Backplane when removing or replacing the card cage, do not scrape it against the CPU heat sink as you move the card cage into or out of the chassis.

Step 2. Grasp the flat lever handle on the right side of the Card Cage and pull it up and out of the way. Align the I/O Backplane card connector with the System Board receiver and push in firmly to seat it. Push the flat lever handle down flush with the top of the Card Cage.

Step 3. Secure the two captive Phillips-head screws located at the front of the Card Cage.

Step 4. Replace the I/O card attached to the right side of the I/O Card Cage (slot 1) on the I/O Backplane as follows:

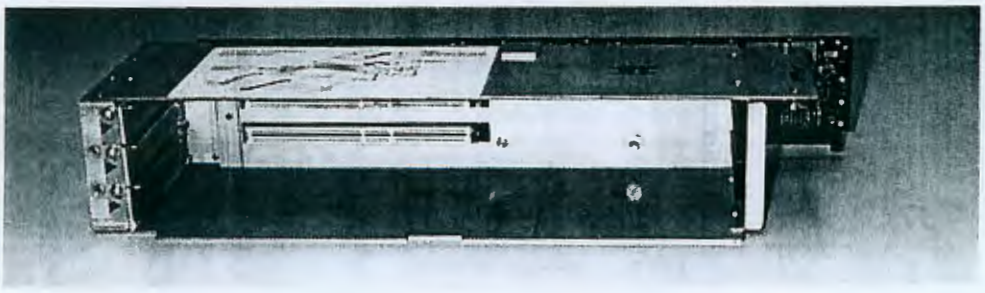
a. Seat the I/O Card into its slot on the I/O Backplane.

b. Replace the screw that attaches the I/O card to the rear bulkhead.

NOTE A short-shaft or right-angle Phillips-head screwdriver must be used to replace the screw due to the short distance between the screw head and the right side of the chassis.

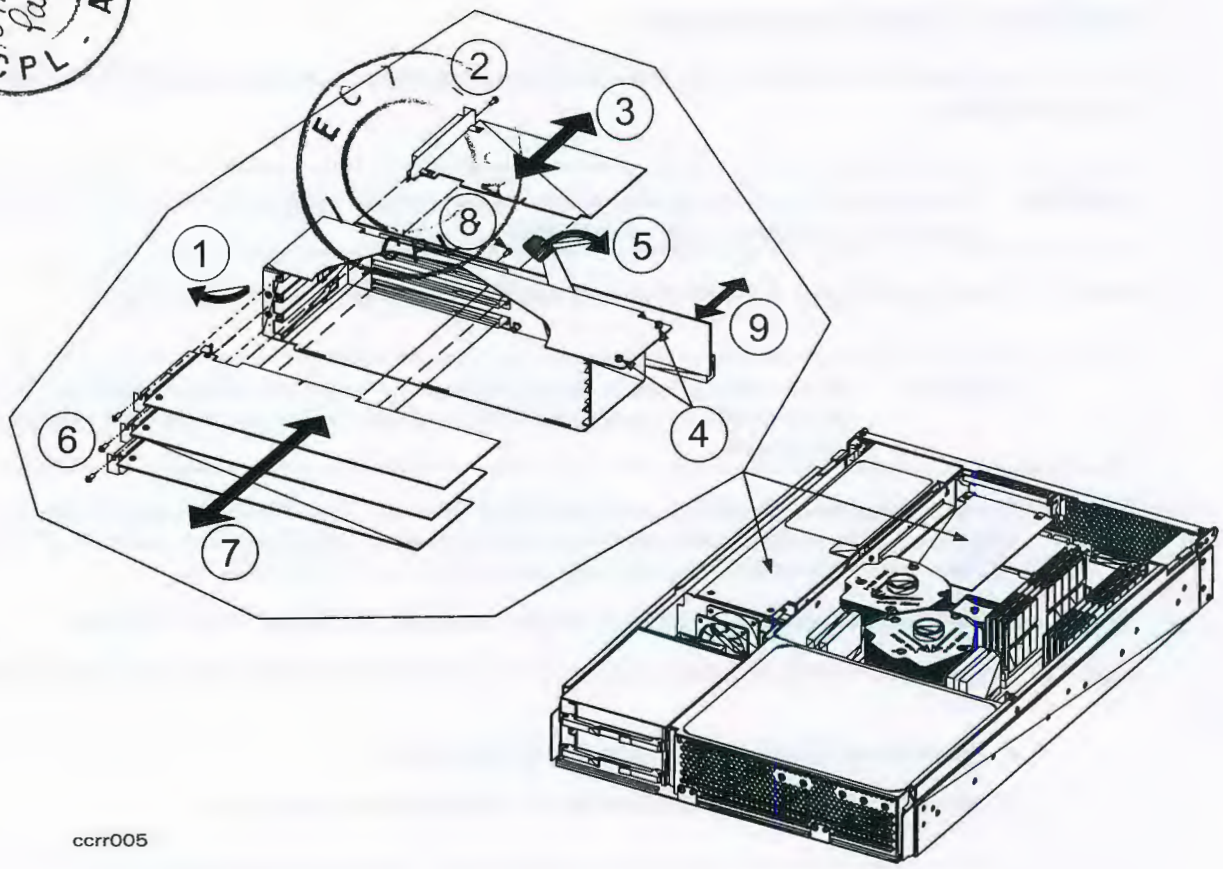
c. If the card in slot 1 is a Secure Web Console card, plug the 5V power connector into the receptacle on the Guardian Service Protector card.

The following photograph shows an empty I/O Card Cage.



The following graphic shows the components of an I/O Card Cage.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 701
Doc. 3698



ccrr005

No.	Title
1	I/O Card Cage
2	I/O Card #1 slot tab
3	I/O Card #1 (short card only)
4	Top front captive screws
5	Flat lever handle
6	I/O Cards #2 through 4 slot tabs
7	I/O Cards #2 through 4 (long or short cards)
8	I/O Backplane retainer screw
9	I/O Backplane

PCI I/O Card Removal

PCI slots 2, 3, and 4 are located in the I/O Card Cage, which must be taken out of the chassis prior to removing these cards. PCI slot 1 supports a short PCI I/O card attached to the I/O Backplane and is located outside of the card cage If a Secure Web Console card was ordered as part of the system, it may be located in this slot and must be removed before taking the I/O Card Cage out of the chassis.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component. Always use an antistatic wrist strap and mat when working on the server.

Remove PCI I/O cards as follows:

- To remove PCI I/O card 1:
  a. Remove the screw that fastens the connector to the inside bulkhead.
  b. Pull the I/O card out of its slot on the outside I/O Backplane.

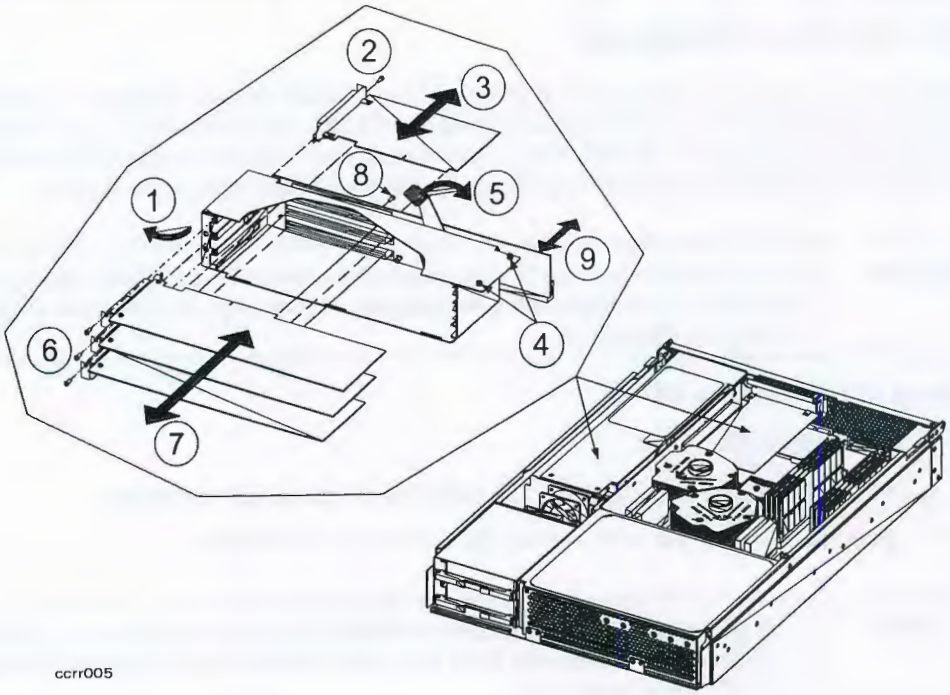
NOTE If you are removing the Secure Web Console card in the slot 1 position, ensure that the 5v power plug is removed from the power outlet (located on the Guardian Service Processor (GSP), front right side).

- To remove PCI I/O cards 2, 3, and 4:
  a. Take the I/O card cage out of the server.
  b. Grasp the edge of the I/O card and pull it out of its slot in the card cage.

The following graphic shows an exploded view of the I/O card cage with I/O cards.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 3698
Doc.

ECT
CPL. AC



No.	Title
1	I/O Card Cage
2	I/O Card #1 slot tab
3	I/O Card #1 (short card only)
4	Top front captive screws
5	Flat lever handle
6	I/O Cards #2 through 4 slot tabs
7	I/O Cards #2 through 4 (long or short cards)
8	I/O Backplane retainer screw
9	I/O Backplane

PCI I/O Card Replacement

PCI slots 2, 3, and 4 are located in the I/O Card Cage, which must be taken out of the chassis prior to replacing these cards. PCI slot 1 supports a short PCI I/O card attached to the I/O Backplane and is located outside of the card cage. If a Secure Web Console card was ordered as part of the system, it may be located in this slot and must be replaced after reinstalling the I/O Card Cage in the chassis.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component. Always use both an ESD antistatic wrist strap and and ESD mat when working on the server.

To replace PCI I/O cards, proceed as follows:

- To replace PCI I/O cards 2, 3, and 4:

NOTE If a PCI card is installed in slot #1 (outside of the I/O card cage), it must be removed before the card cage can be removed from the server.

  a. Take the I/O card cage out of the server.
  b. Orient the replacement I/O card in its guide slot and push it into the card cage until the card connector seats in the I/O Backplane.
  c. Replace the screw that fastens the I/O connector to the bulkhead.

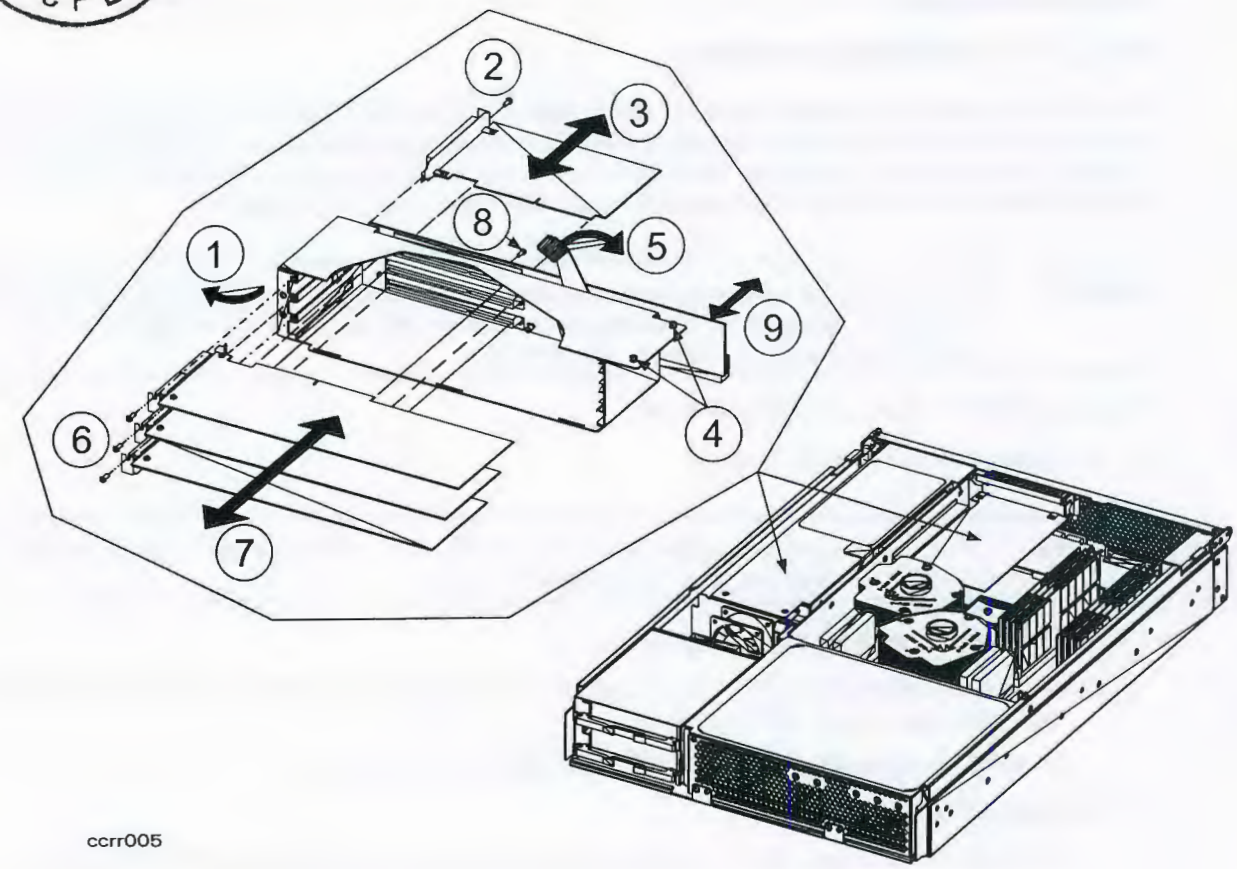
- To replace PCI I/O card 1:

  a. Push the I/O card into its slot until the card connector seats in the outside I/O Backplane.
  b. Replace the screw that fastens the connector to the inside bulkhead.

NOTE If you are replacing the Secure Web Console card, ensure that the 5v power plug is seated into power outlet (located on the Guardian Service Processor, front right side) after the card is installed.

The following graphic shows an exploded view of the I/O card cage with I/O cards.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 769
3698
Doc.



ccrr005

No.	Name	No.	Name
1	I/O Card Cage	6	I/O Card anchor screws
2	Outside I/O Card anchor screw	7	I/O Cards #2 through #4
3	Short I/O Card #1 (may be Secure Web Console)	8	I/O Backplane anchor screw
4	I/O Card Cage anchor quarter-turn fasteners	9	I/O Backplane
5	I/O Backplane disconnect lever		

PCI Backplane Removal

The PCI backplane is located on the back of the I/O Card cage. I/O slot 1 is located on the outside of the PCI I/O card cage and slots 2, 3, and 4 are attached to the PCI backplane inside the I/O card cage.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To remove the PCI backplane from the server, perform the following steps:

Step 1. Remove the I/O cables from the back of the server.

Step 2. Remove the I/O card from slot 1.

Step 3. Remove the I/O card cage from the server.

CAUTION Do not scrape the I/O Backplane against the CPU heat sink when removing or replacing the card cage. Failure to heed this precaution could cause serious damage to the backplane and require replacement.

Step 4. Remove all PCI cards.

NOTE Note the order of PCI card installation prior to removal. Cards must be re-installed in the same slots, or I/O reconfiguration may be required.

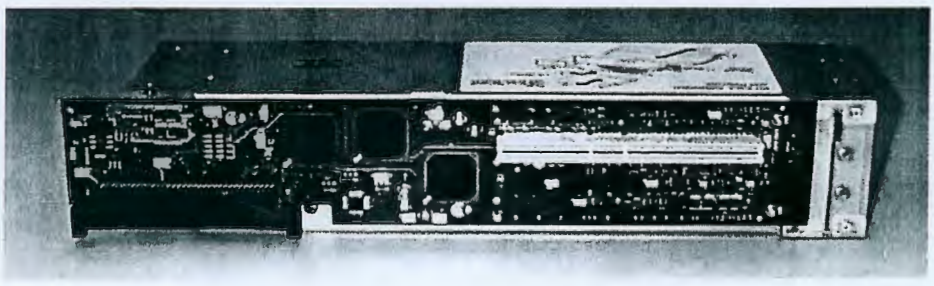
Step 5. Lay the I/O card cage, open side down, on a clean, dry surface. The PCI backplane is facing up.

Step 6. Remove the T-10 retainer screw from the PCI backplane.

Step 7. Slide the PCI backplane to one side, so that the retainer posts will clear the keyhole slots.

Step 8. Grasp the PCI backplane by the edges and carefully remove it from the card cage.

The following photograph shows the PCI Backplane.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 701
3698
Doc.

ECT 8904 CPL - AC

PCI Backplane Replacement

The PCI backplane is located on the back of the I/O Card cage. I/O slot 1 is located on the outside of the PCI I/O card cage and slots 2, 3, and 4 are attached to the PCI backplane inside the I/O card cage.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To replace the PCI backplane, perform the following steps:

Step 1. Lay the I/O card cage, open side down, on a clean, dry surface. When installed, the PCI backplane will be facing up.

Step 2. Grasp the PCI backplane by the edges and carefully set it on the card cage retainer posts.

Step 3. Slide the PCI backplane to one side so that the retainer posts lock into the keyhole slots.

Step 4. Replace the T-10 retainer screw that secures the PCI backplane to the card cage.

Step 5. Replace all PCI cards.

NOTE PCI Cards must be re-installed in the same slots from which removed, or I/O reconfiguration may be required.

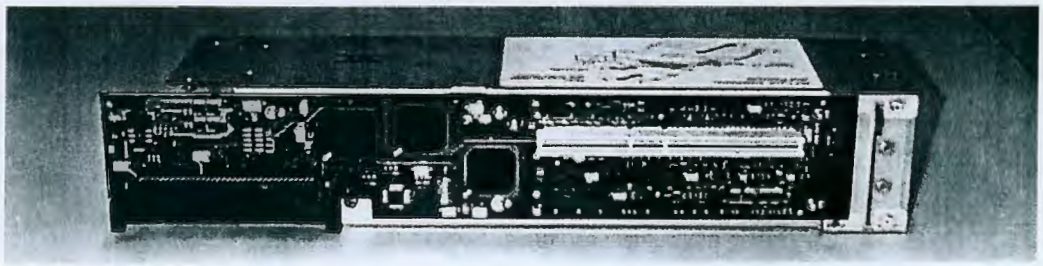
Step 6. Replace the I/O card cage into the server.

CAUTION Do not scrape the I/O Backplane against the CPU heat sink when removing or replacing the card cage. Failure to heed this precaution may cause serious damage to the backplane.

Step 7. Replace the I/O card in slot 1.

Step 8. Attach the I/O cables to the back of the server.

The following graphic shows the PCI Backplane.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 705
3698
Doc.

E C T
8905 Paula
C P L - A

DC-DC Converter Removal

DC-DC Converter boards and slave boards are required to power each CPU.

CPU MHz	Master	Slave
440	1	1
550*	1	2
* When available		

NOTE Each CPU requires a DC-DC Converter and slave(s) to operate. When upgrades are performed on the CPU, change the accompanying DC-DC Converter and slave(s) also. When returning replaced CPUs, return the accompanying DC-DC Converter and slave(s) also.

The converter boards stand on edge in slots and are located immediately behind the Power Supply on the left and right sides of the System Board, next to the CPU assemblies.

CAUTION DC-DC converter boards are not "hot-swap" or "hot-plug" units. Shut the server down and unplug the electrical connection prior to removing or replacing DC-DC converter boards.

To remove a DC-DC Converter board and its slave(s) from the server, perform the following steps:

Step 1. Gently pull the left and right levers away from each side of the board approximately 0.635 cm (1/4 in.).

CAUTION DO NOT press hard on the left/right levers or they will break. The levers do not extract the board from its socket. They provide vertical stability, only.

Step 2. Grasp the board by the left and right edges.

Step 3. With a gentle rocking motion, pull the board up and out of its slot.

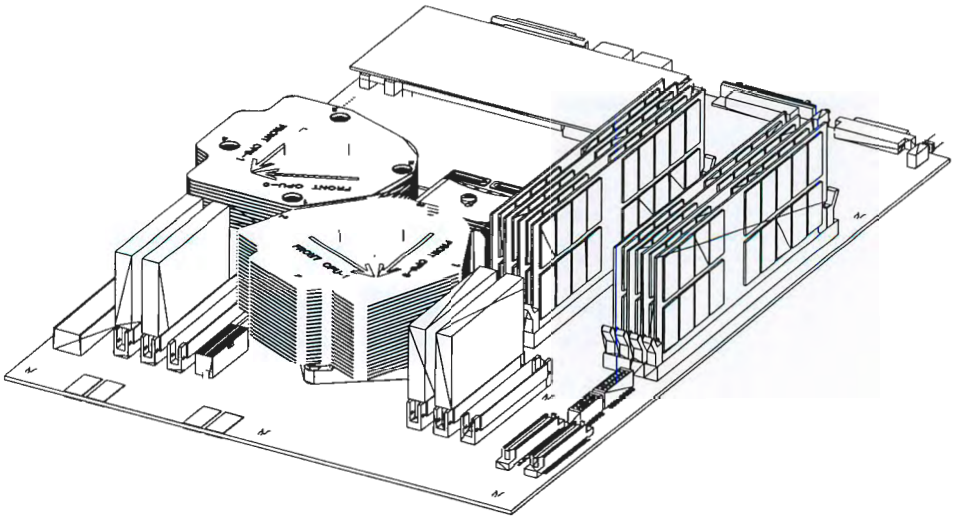
Step 4. Place the board on a clean, static-free surface.

CAUTION There is little working room between the DC-DC converter boards and slave(s) and CPU-1. If necessary, use a flat-blade screw driver to reach and release the levers prior to removing these boards.

The following graphic shows the location of the DC-DC converter boards and slaves.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 706
3698
Doc.

ECT
CPL - AC



DC-DC Converter Replacement

DC-DC Converter boards and one or two slave boards (depending on the CPU speed) are required to power each CPU.

CPU MHz	Master	Slave
440	1	1
550*	1	2
* When available		

NOTE Each CPU requires a DC-DC Converter and slave(s) to operate. When CPUs are upgraded or replaced, ensure that the accompanying DC-DC Converter and slave(s) are changed. When returning replaced CPUs to Hewlett-Packard, ensure that the accompanying DC-DC Converter and slave(s) are returned also.

The converter boards stand on edge in slots and are located immediately behind the Power Supply on the left and right sides of the System Board, in front of the CPU assemblies.

CAUTION DC-DC converter boards are not "hot-swap" or "hot-plug" units. Shut the server down and unplug the electrical connection prior to removing or replacing DC-DC converter boards.

To replace a DC-DC Converter board and its slave(s) from the server, perform the following steps:

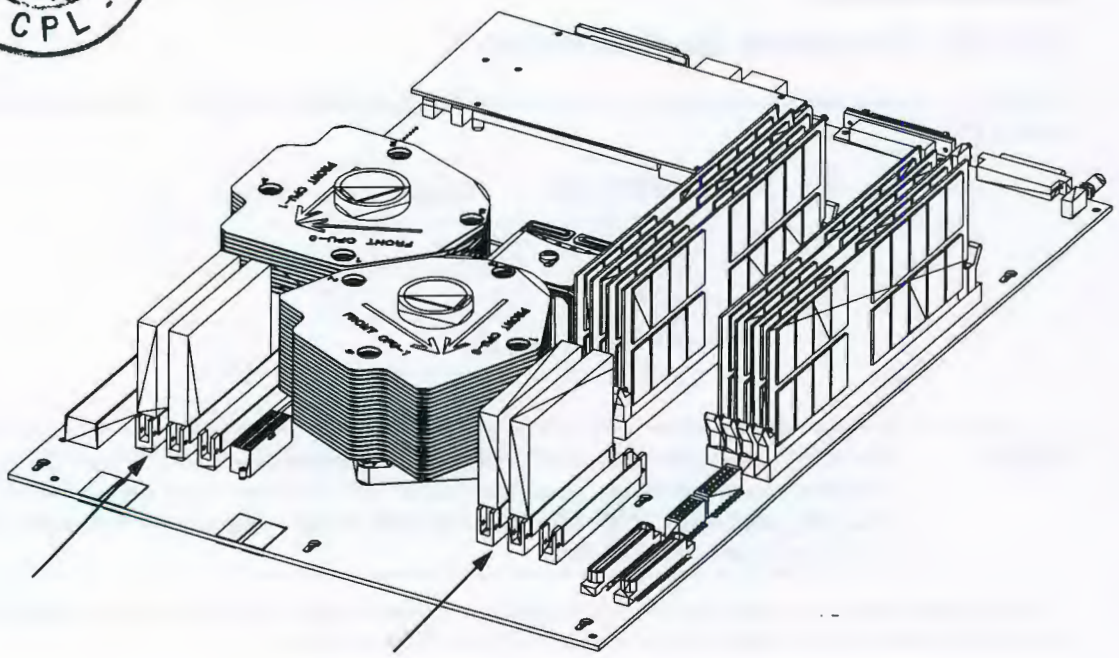
Step 1. Grasp the board by the left and right edges.

Step 2. Align the board connector with the slot. The slot and board are keyed so that the board will only fit one way. Place your thumbs on the top edge of the board, near the left and right sides, and push the board straight down into its slot until either an audible "click" is heard, or the levers close and seat into the slots in the side edges of the board

CAUTION DO NOT press hard on the left/right levers or they will break. Levers provide vertical stability, only.

The following graphic shows a DC-DC converter board and slave(s).

RQS nº 03/2005 - CN
CPMI - CORREIOS
707
Fls Nº
3698
Doc.



ccrr010

Memory DIMM Removal

Memory DIMMs reside in eight sockets (two sets of four sockets each) located on the right side of the System Board. They are normally loaded in DIMM pairs of equal size.

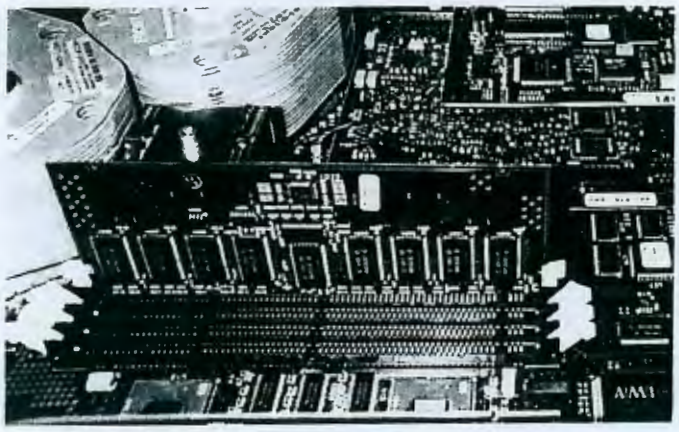
CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

To remove a memory DIMM, perform the following steps:

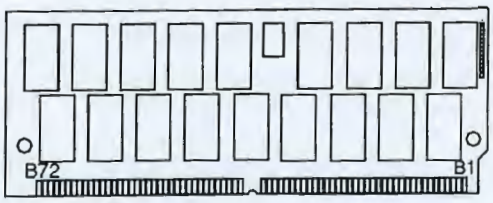
Step 1. Press down on the extractor levers on each end of the selected memory DIMM to unseat the DIMM from its socket.

Step 2. When the DIMM is unseated, pull it up and out of the System Board.

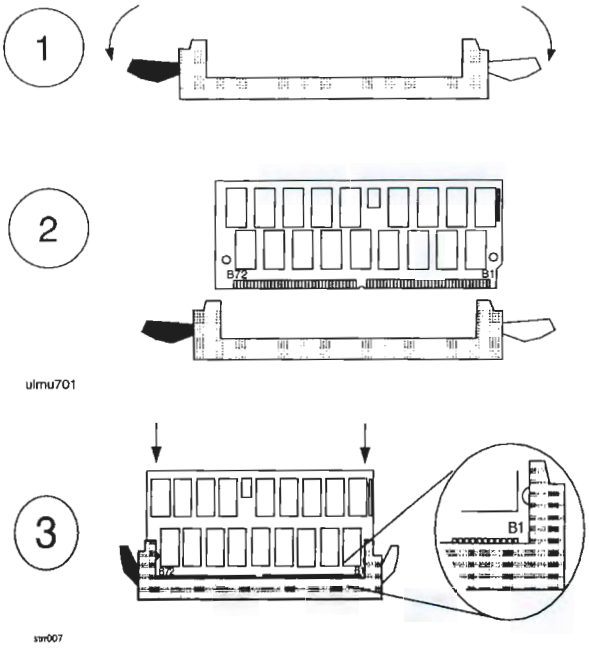
The following picture shows a memory DIMM located on the right side (from the server front) of the server system board.



The next graphic is a drawing of a generic memory DIMM, followed by drawings that show DIMM removal/replacement.



Memory DIMM Removal



ECT 8894 Paula CPL - AC

Memory DIMM Replacement

Memory DIMMs reside in sockets located on the right side (from the front) of the System Board.

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

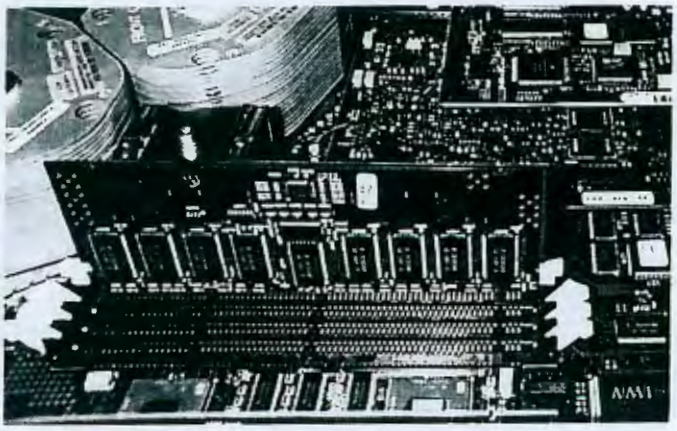
To replace a memory DIMM, perform the following steps:

CAUTION Be careful to insert the DIMM into the socket evenly. Do not rock the DIMM when seating it.

Step 1. Match the guide slots on the bottom of the DIMM with the guides on the socket and seat the memory DIMM into the socket. Insert the DIMM connectors into the guides until the card snaps firmly in place. It may be necessary to apply downward force using the palm of your hand on the DIMM. Ensure that one side the DIMM is not higher than the other.

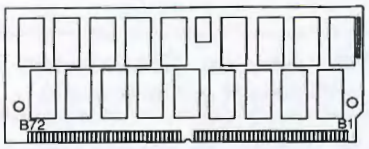
Step 2. Use the BCH command `in me` to verify that the system recognizes the memory that you have just replaced.

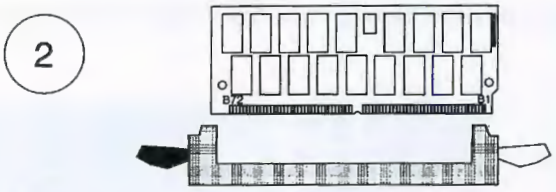
The following picture shows the memory DIMMs located on the right side (from the server front) of the server system board.



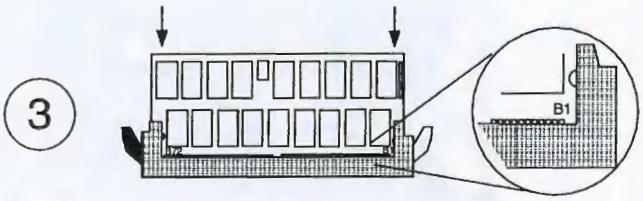
The following graphic is a drawing of a generic memory DIMM, followed by drawings that show DIMM removal/replacement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 709
Doc.





ulmu701



str007

ECT - CPL - AC 8894 Paulo

Guardian Service Processor (GSP) Removal

The GSP card resides on the System Board at the rear left center, under the short PCI I/O card (slot 1), which must be removed for access.

Before removing the GSP from the server, perform the following steps:

CAUTION Ensure that the system is shut down and power removed from the server before attempting removal or replacement of a component.

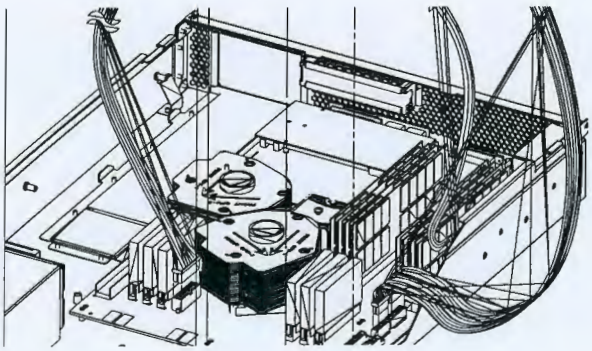
To remove the GSP from the server, perform the following steps:

Step 1. Loosen the four mounting screws that hold the GSP card in place.

Step 2. Grasp the card by the left and right edges, rock it gently to free it from its socket on the System Board, and lift it out of the server.

The following picture shows the a GSP installed in a server.

The following graphic shows the location of a GSP in the server.

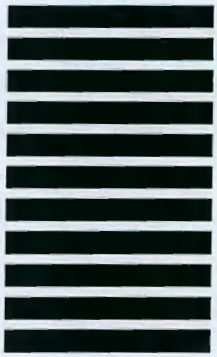


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 710
3690
Doc.

Apêndice IF

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1711
Doc. 3698

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 256 ROSEVILLE, CA

POSTAGE WILL BE PAID BY ADDRESSEE

Attention: Information Engineering (MS5668)

Hewlett-Packard Company
HP Storage Organization/ MSO
8000 Foothills Boulevard
Roseville, CA 95747-9987

Fold Here

Please Do Not Staple

Tape

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 712
Doc.

Reader Comment Sheet

Hewlett-Packard SureStore Disk System 2100 User Guide

We welcome your evaluation of this manual. Your comments and suggestions will help us improve our publications. Remove this page and mail or FAX it to 916-785-2299. Use and attach additional pages if necessary.

	Agree				Disagree	N/A
The manual is well organized.	○	○	○	○	○	○
The information is technically accurate.	○	○	○	○	○	○
Information is easy to find.	○	○	○	○	○	○
Step-by-step procedures are easy to perform.	○	○	○	○	○	○
There are enough examples and pictures.	○	○	○	○	○	○
The examples and pictures are useful.	○	○	○	○	○	○

Comments _____

_____

_____

_____

Name: _____ Phone: _____

Title: _____ FAX: _____

Company: _____ E-mail: _____

Address: _____ ZIP: _____

City & State: _____ Country: _____

___ Check here if you would like a reply.

Hewlett-Packard has the right to use submitted suggestions without obligation, with all such ideas becoming the property of Hewlett-Packard.

HPSO/MSO Roseville Information Engineering

A5675-90901 E0301

Product Web Site

This guide is available in Adobe® Acrobat® format on the HP Customer Care web site for enterprise storage (*http://www.hp.com/essd/*). The complete URL is *www.hp.com/support/ds2100*

Related Documents

The following manuals explain how to use the system software interfaces to the HP Surestore Disk System 2100:

- *Online Diagnostics (for HP 9000): Support Tools Manager Overview*, available at *http://www.docs.hp.com/hpux/systems/*
- *HP-UX System Administration Tasks Manual*, HP Order No. B2355-90079
- Window's NT installation guide for HP Netservers: (NT 4.0) *http://netserver.hp.com/netserver/docs/download.asp?file=it_nt_5_5_00.pdf*
- Window's NT installation guide for HP Netservers: (NT 2000) *http://netserver.hp.com/netserver/docs/download.asp?file=it_win2k_5_1_00.pdf*
- Window's NT installation guide for Legacy HP Netservers: (NT 4.0) *http://netserver.hp.com/netserver/docs/download.asp?file=ig_mwnt40.pdf*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 713
Doc. 3698

DECLARATION OF CONFORMITY
according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747
USA

declares, that the product

Product Name: HP SureStore Disk System 2100

Model Number(s): A5675A, A5675AD, A5675AZ, A5676A, A5676AD

Product Options: All

conforms to the following Product Specifications:

Safety: IEC 950:1991 + A1, A2, A3, A4 / EN 60950:1992 + A1, A2, A3, A4, A11
GB 4943-1995

EMC: CISPR 22:1997 / EN 55022:1998 Class A[1]
GB 9254-1988
CISPR 24:1997 / EN 55024:1998
IEC 61000-3-2:1995 / EN 61000-3-2:1995
IEC 61000-3-3:1994 / EN 61000-3-3:1995
FCC Title 47 CFR, Part 15[2]

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The product was tested in a typical configuration with a Hewlett-Packard computer system and peripherals.
2) The product complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
   - this device may not cause harmful interference; and
   - this device must accept any interference received, including interference that may cause undesired operation.

Roseville, December 6 , 2000

Frank L. Sindelar, NSSO Regulatory Mgr.

North American Contact: Hewlett-Packard Company Product Regulations Manager, 3000 Hanover Street, Palo Alto, CA 94304 Phone: 650-857-1501

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE, Herrenberger Straße 130, D-71034 Böblingen (FAX: + 49-7031-14-3143)

C. Notice for Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。
取り扱い説明書に従って正しい取り扱いをして下さい。

Harmonics Conformance (Japan)

高調波ガイドライン適合品

D. Notice for Taiwan

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

E. Notice for Korea

사용자 안내문 (B급 기기)

이 기기는 비업무용으로 전자파장해검정을 받은기기로서, 주거지역에서는 물론 모든 지역에서 사용 할 수 있읍니다.

F. Notice for Germany

Schalldruckpegel Lp = 55.0 dB(A)

Am Arbeitsplatz (operator position)

Normaler Betrieb (normal operation)

Nach ISO 7779:1999 (Typprüfung)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 714
Doc. 3698

E C T
8360
Paula
C P L - A C

Japan: VCCI Class B

Taiwan: CNS 13438, Class A

US: 47 CFR Parts 2 & 15, Class B

A. FCC Notice for United States

The Federal Communications Commission (in 47 CFR 15.105) has specified that the following notice be brought to the attention of the users of this product.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antennna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Hewlett-Packard's cerification tests were conducted with a Hewlett-Packard supported computer system and Hewlett-Packard shielded cables, such as those you received with your storage product. Changes of modificaitons not expressly approved by Hewlett_packard could void the user's authority to operate the equipment. cables used with this device must be properly sheilded to comply with the requirements of the FCC.

B. FCC Notice for Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

TABLE 16 Environmental Specifications

Climate Control		
Temperature (dry bulb)	Operating	0°C - +40°C
	Storage	-40°C - +70°C
Relative Humidity (non-condensing)	Operating	5% - 95% Relative Humidity at 40°C
	Storage	90% Relative Humidity at 65°C
Altitude (based on disks)	Operating	-1000 ft to +10,000 ft (3048 M)
	Storage	40,000 ft (12,092 M)
Heat Dissipation (maximum)	Operating	< 100 watts

Operating Temperatures

If the storage system is installed in a multi-unit rack assembly, the operating ambient temperature of the rack environment may exceed room ambient temperature. The rack environment ambient temperature cannot exceed 40° Celsius (104° Fahrenheit).

If your storage system contains less than 4 disk modules, the remaining empty slots require filler panels. These filler panels (part number A6198-60001) ensure that the proper cooling is maintained within the storage system.

Regulatory Statements

Safety Certifications

UL listed, UL 1950:1995 – 3rd Edition

CSA certified, C22.2 No. 950:1989

TUV certified with GS mark, EN 60950:1992 + A1:1993, A2:1993, A3:1995, A4:1997

CE mark (see on page 39)

EMC Compliance

Australia: AS/NZS 3548, Class B

Canada: ICES-003, Class B

China: GB9254-88

European Union: EN55022 Class B, EN55024

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 715
3608
Doc.

E C T
CPL - AC

TABLE 13 Supported HP Cables and Terminators (for Commercial Systems)

Order Number	Description	Part Number
A6523A	0.5-meter HDT S68 SCSI multimode cable	5183-2670
A6524A	1.0-meter HDT S68 SCSI multimode cable	5183-2671
A6525A	1.5-meter HDT S68 SCSI multimode cable	5183-2672
A6526A	2.5-meter HDT S68 SCSI multimode cable	5183-2673
A6527A	5.0-meter HDT S68 SCSI multimode cable	5183-2678
A6528A	1.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2674
A6529A	2.5-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2675
A6530A	5.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2676
A6531A	SCSI Terminator LVD/SE HDTS68	5183-2657

Specifications

TABLE 14 Physical Dimensions

Measure	Metric	English
Width	45.08 cm	17.75 in
Depth	38.10 cm	15.0 in
Height	4.32 cm	1.7 in
Weight without disk modules	4.94 kg	10.90 lbs
Weight fully loaded	8.11 kg	17.89 lbs

Electrical Specifications

TABLE 15 AC Power Requirements

Electrical Element	Requirement
AC Operating Voltage Range	88-269 VACRMs
Line Frequency Range	47-63 Hz
Published Product Operating Range	100 - 240 VACRMs
Published Product Frequency Range	50 - 60 HZ

E C T
8863
Paula
CPL - AC

TABLE 11 Replaceable Parts

Product Number	Description	Replaceable Part Numbers
A5675A	Base Disk System Assembly	A5675-67001
A6198A	Disk Filler Panel	A6198-60001
A6537A	18-Gbyte 10,000 rpm LVD disk module	A6537-69001
A6538A	36-Gbyte 10,000 rpm LVD disk module	A6538-69001
A6544A	18-Gbyte 10,000 rpm LVD disk module	A6544-69001
A6545A	36-Gbyte 10,000 rpm LVD disk module	A6545-69001
	Desktop Disk System Cover	5065-5217
	Desktop Disk System Feet	0403-0285

TABLE 12 Supported HP Cables and Terminators (for Enterprise Systems)

Order Number	Description	Part Number
C2978B	0.5-meter HDT S68 SCSI multimode cable	5183-2670
C2911C	1.0-meter HDT S68 SCSI multimode cable	5183-2671
C2979B	1.5-meter HDT S68 SCSI multimode cable	5183-2672
C2924C	2.5-meter HDT S68 SCSI multimode cable	5183-2673
C7521A	5.0-meter HDT S68 SCSI multimode cable	5183-2678
C2361B	1.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2674
C2362B	2.5-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2675
C2365B	5.0-meter VHDT S68/HDT S68 SCSI multimode cable	5183-2676
C2364A	SCSI Terminator LVD/SE HDTS68	5183-2657

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 716
Doc. 3698

E C T
8864
C P L - A C

Upgrade Disk Products Available

TABLE 9 Available Upgrade Disk Modules

Product Number	Description
A6537A	18-Gbyte 10,000 rpm LVD disk module (for Enterprise Systems)
A6538A	36-Gbyte 10,000 rpm LVD disk module (for Enterprise Systems)
A6544A	18-Gbyte 10,000 rpm LVD disk module (for Commerial Systems)
A6545A	36-Gbyte 10,000 rpm LVD disk module (for Commerial Systems)

TABLE 10 Upgrade Products for Hewlett-Packard Systems

Product Number	Description
A4999A	Single Port Ultra 2 SCSI Host Bus Adapter for Hewlett-Packard Workstations
A5149A	Single Port Ultra 2 SCSI Host Bus Adapter for HP-UX Systems
A5150A	Dual Port Ultra 2 SCSI Host Bus Adapter for HP-UX Systems
A5856A	Internal Disk Array Controller for HP-UX Systems
A5675A	HP Surestore Disk System 2100
A5679A	Rail kit for the Rittal Style Rack Systems and HP Rack Systems/E
A5680A	Rail kit for HP Rack Systems
A6198A	Disk Filler Panel
C2364A	LVD/SE SCSI Terminator (HDTS68)
C7430A	Ultra 2 SCSI Host Bus Adapter for HP Netservers
D2140A	Netraid 1si Host Bus Adapter for HP Netservers
D5025A	Ultrawide Host Bus Adapter for HP Netserver
D5955A	Netraid 3si Host Bus Adapter for HP Netservers
D9161A	Netraid 4M/64 Host Bus Adapter for HP Netservers
D9351A	Netraid 4M/128 Host Bus Adapter for HP Netservers
P3413A	Single Port Ultra 3 SCSI Host Bus Adapter for HP Netservers

Reference Information

Product Numbers and Options

Three models of the disk system are available:

- A5675A field-racked disk system (Enterprise Customer Installable)
- A5675AD desktop disk system (Enterprise Systems)
- A5675AZ factory racked disk system (Enterprise Systems)
- A5676A field-racked disk system (Commerial Customer Installable)
- A5676AD desktop disk system (Commerial Systems)

TABLE 8 Products and Options

Disk System Product Number	Disk Module Product (with Option)	Description
A5675A		Field installed disk system (Enterprise)
	A6537A (0D1)	Drive integrated into the field installed disk system
	A6538A (0D1)	Drive integrated in the same field installed disk system
A5675AD		Desktop disk system (Enterprise)
	A6537A (0D1)	Drive integrated into the factory installed disk system
	A6538A (0D1)	Drive integrated in the same factory installed disk system
A5675AZ		Factory installed disk system (Enterprise)
	A6537A (0D1)	Drive integrated into the desktop disk system
	A6538A (0D1)	Drive integrated in the same desktop disk system
A5676A		Field installed disk system (Commercial)
	A6544A (0D1)	Drive integrated into the field installed disk system
	A6545A (0D1)	Drive integrated in the same field installed disk system
A5676AD		Desktop disk system (Commercial)
	A6544A (0D1)	Drive integrated into the factory installed disk system
	A6545A (0D1)	Drive integrated in the same factory installed disk system

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 71
3696
Doc.

ECT CPL - AC

Isolating Faults

Table 7 lists the probable causes and solutions for problems you may detect on the disk system. When more than one problem describes your situation, investigate the first solution that applies. The table lists the most basic problems first and excludes them from subsequent problem descriptions.

Erratic LED behavior on the disk system could be observed in the following situations:

- When a server that is connected to a Disk System 2100 is powered down or loses power (and the disk system remains powered on)
- When the disk system is powered up when connected to a downed server
- When an unconnected disk system is powered up

An example of this LED behavior is the LEDs staying lit solidly. This condition is caused by the disk system being deprived of term power when the server loses power or is powered down. The disk system does not provide its own term power. It relies on the host bus adapter to which it is connected for term power.

TABLE 7 Troubleshooting Table

Problem Description	LED State	Probable Cause/Solution
Disk system fails to power on when installed	System power LED is off	Power cord is not plugged in. The power button is not pressed. AC breaker is tripped or AC power source has failed. The PDU/PDRU is defective. Replace. Enclosure chassis is faulty. Replace.
	System power LED is blinking	Power supply is defective - replace the enclosure Cooling fans are not spinning at the correct speed - replace the enclosure.
Operating system reports errors on a device	Disk module LED is on solid or off	Use diagnostic utilities to determine disk status. Depending on the results, monitor or replace disk module.
IOSCAN (HP-UX) lists disk as NO_HW, or Mapper or DSTAT ALL (MPE/iX) lists no device type	Disk module LED is on solid or off	Disk module is faulty - Replace. Enclosure is faulty - Replace. If the all disks on the bus have this problem, the cable is faulty. Replace the cable.
Unable to configure device for use by operating system	Disk module LED is on solid or off	Disk module possibly not correctly seated. If at a new installation, remove and reinstall the disk module. If troubleshooting an existing installation, run diagnostics to determine drive status. Replace the disk module.

ECT 8864 Paulo CPL. AC

FIGURE 16 Sample STM Expert Tool Disk Error Log (MPE/iX 6.5 or 7.0)

```
Write Error Statistics

    Errors Corrected Without Delay:   N/A
    Errors Corrected With Delay:      0
    Total Retries:                    0
    Total Errors Corrected:           0
    Correction Algorithm Executions:  0
    Total Bytes Processed:            6.3253e+10
    Total Uncorrected Errors:         0

Read Error Statistics

    Errors Corrected Without Delay:   23781
    Errors Corrected With Delay:      0
    Total Retries:                    0
    Total Errors Corrected:           23781
    Correction Algorithm Executions:  23781
    Total Bytes Processed:            9.6191e+10
    Total Uncorrected Errors:         0

Read Reverse Error Statistics

    Errors Corrected Without Delay:   N/A
    Errors Corrected With Delay:      N/A
    Total Retries:                    N/A
    Total Errors Corrected:           N/A
    Correction Algorithm Executions:  N/A
    Total Bytes Processed:            N/A
    Total Uncorrected Errors:         N/A

Verify Error Statistics

    Errors Corrected Without Delay:   0
    Errors Corrected With Delay:      0
    Total Retries:                    0
    Total Errors Corrected:           0
    Correction Algorithm Executions:  0
    Total Bytes Processed:            36864
    Total Uncorrected Errors:         0

Non-Medium Error Counts:              0
```

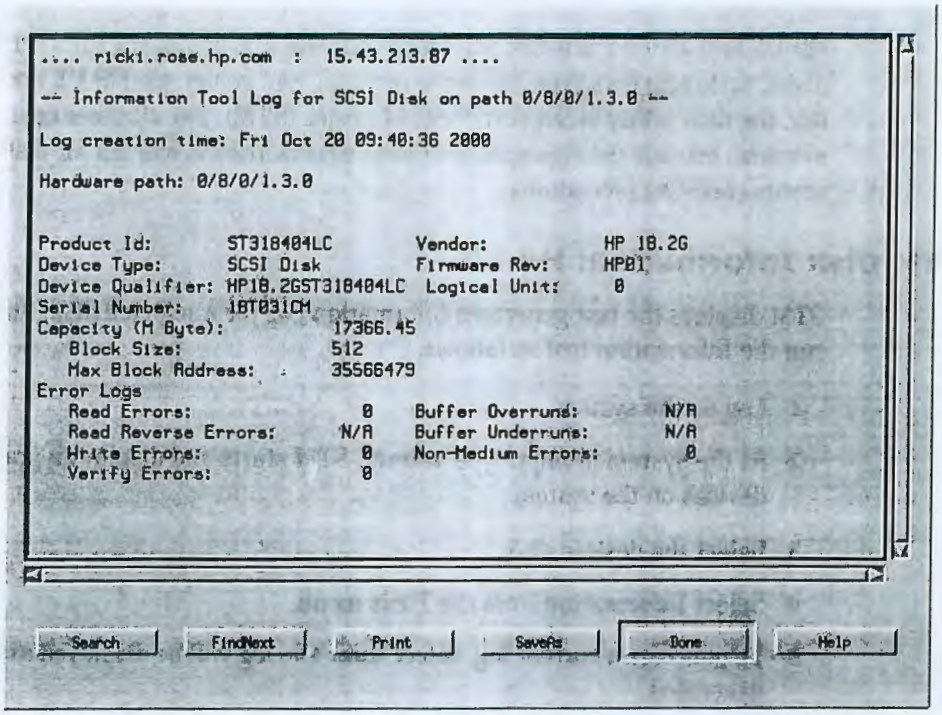
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 718
Doc. 3698

STM Disk Information: MPE/iX 6.5 or 7.0

STM displays the last-generated Information Log for a selected disk. Start STM and run the Information tool as follows.

1. Log on the system.
2. At the system prompt (:), type **vsclose** <physical volume number>. This removes the disk from use.
3. At the system prompt (:), type **cstm**. STM starts.
4. At the cstm prompt, type **map**. STM displays a list of all the disks installed on the system.
5. Select the desired disk by typing **select device** <number>; for example, **select device 15**.
6. Type **information**. STM updates the system map.
7. To display the information log, type **infolog**.

FIGURE 15 Sample STM Information Log (HP-UX)



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 719
Doc. 3698

ECT CPL - AC

View Disk Status

HP-UX and MPE/iX utilities provide descriptive and diagnostic information about disks, including disk type, firmware revision, and errors. On HP-UX and MPE/iX 6.5, the disk utility is Support Tools Manager (STM). For all other operating systems, consult the appropriate system administration manual for disk module status checking procedures.

STM Disk Information: HP-UX

STM displays the last-generated Information Log for a selected disk. Start STM and run the Information tool as follows.

1. Log on the system.
2. At the system prompt, type **xstm&**. STM starts and displays a graphic of the devices on the system.
3. Select the desired disk.
4. Select **Information** from the Tools menu.
5. To generate a current log, select **Run**. The log will be displayed as soon as it is generated
6. To view a log without updating the contents, select **Information Log**.
7. Select **Done** when you have finished viewing the information.
8. To quit STM, type **exit**.
9. Figure 15 shows a sample Information Log.

Status LEDs

LEDs indicate the status of the disk system itself and each of the disk modules. A green system LED is visible on the front of the disk system. It shows that a fault has occurred or that power is on. Disk activity LEDs are on the front of the disk modules (see Figure 14 and Table 6 below).

FIGURE 14 LED Status Indicators

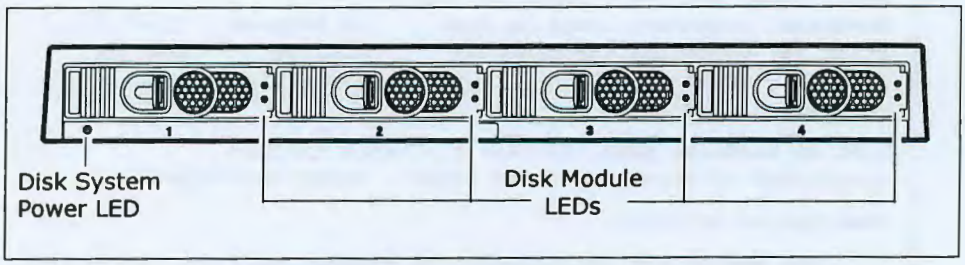


TABLE 6 LED Status Indicators

LED	State	Indication
System Power	Green	Power is on
	Blinking	Malfunction - either a fan is not operating properly or internal voltage is too low.
	OFF	Power is off
Disk Activity	ON	Installed and spinning up. If the LED is still on 3 minutes after power is engaged, the disk may be faulty.
	Flashing	I/O activity on the disk
	OFF	Not installed, not operating, or no I/O activity

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 720
3698
Doc.

ECT CPL - AC 8872 Lavia

FIGURE 13 Sample Hardware Event Notification

```
Notification Time:  Wed Feb 3 11:27:15 1999

yourserver sent Event Monitor notification information:

/storage/events/disks/default/10_4_4_0.0 is >=1.
Its current value is CRITICAL(5)

Event data from monitor:

Event Time: Wed Feb 3 11:27:15 1999
Hostname: yourserver.rose.hp.com       IP Address : 15.43.213.13
Event ID: 0x0036b8a313000000002        Monitor    : disk_em
Event # : 100037                       Event Class: I/O
Severity : CRITICAL

Disk at hardware path 10/4/4/0.0 : Media failure
Associated OS error log entry id(s) : 000000000000000000

Description of Error:

     The device was unsuccessful in reading data for the current I/
     O request due to an error on the medium. The data could not be
     recovered. The request was likely processed in a way which
     could cause damage to or loss of data.

Probable Cause / Recommended Action:

     The medium in the device is flawed. If the medium is removable,
     replace the medium with a fresh one. Alternatively, if the
     medium is not removable, the device has experienced a hardware
     failure. Repair or replace the device, as necessary.
```

C T
CPL - AC
Paula
3873

Event Notification (HP-UX Only)

The Disk Monitor, an EMS hardware event monitor, reports changes in disk status. Depending on how the monitor is set up, it sends messages to the console, an e-mail address, a log file, or a third-party application. These messages give early notice of a disk problem. Events include media errors, failed read and write attempts, invalid commands, changed operating parameters, failed diagnostics, and many others.

Event severity ranges from critical to informational:

Critical	An event that causes data loss, host system downtime, or other loss of service. Host system operation will be affected if the disk system continues to be used without correction. Immediate action is required. For example, read data could not be recovered.
Serious	An event that may cause data loss, host system downtime, or other loss of service if left uncorrected. Host system and hardware operation may be adversely affected. The problem needs repair as soon as possible. For example, the request queue is full.
Warning	An event that could escalate to a serious condition if not corrected. Host system operation should not be affected and normal use of the disk system can continue. Repair is needed but at a convenient time. For example, the bus failed to reset.
Information	An event that is expected as part of the normal operation of the hardware. No action is required. For example, write protection was switched on or off.

Event messages (see Figure 13) contain the following types of information:

- Message Data – Date and time the message was sent, the source and destination of the message, and the severity level
- Event Data – Date and time of the event, the host, event ID, name of the monitor, event number, event class, severity level, hardware path, associated OS error log entry ID
- Error Description – Narrative information indicating the component that experienced the event and the nature of the event
- Probable Cause/Recommended Action – The cause of the event and suggested steps toward a solution. This information should be the first step in troubleshooting.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 721
3698
Doc.

Setting Up the Hardware Event Monitor (HP-UX Only)

Hardware event monitors run on HP-UX hosts, versions 10.20 and 11.0. The Disk Monitor (disk_em) monitors all disks bound to sdisk drivers. Consequently, if the Disk Monitor is active on your host, it is already set up to monitor the disks of a new disk system. If you need to install or activate the Disk Monitor, refer to the *EMS Hardware Monitors User's Guide* in the latest IPR Support Media or on the Web (*http://www.docs.hp.com/hpux/systems/#ems*)..

> **Note** This Disk Monitor should not be confused with the EMS disk monitor that is used to monitor LVM resources.

The way you configure the monitor determines, among other things, where event messages will be sent and what level of severity will be reported.

Configuration Overview

The following steps will help you identify and resolve disk system failures:

1. Gather information from all sources:
   - Hardware event notifications (page 26)
   - Disk system LED status (page 26)
   - Online information tools (page 27)
2. Isolate the cause of the problem (Table 7 on page 31).
3. Correct the problem. (See page 20 for disk modulecremoval and replacement.)
4. Verify operational status with IOSCAN or other host utilities.

E.T.I. 8845 Paula A.C.

Remove the Disk System

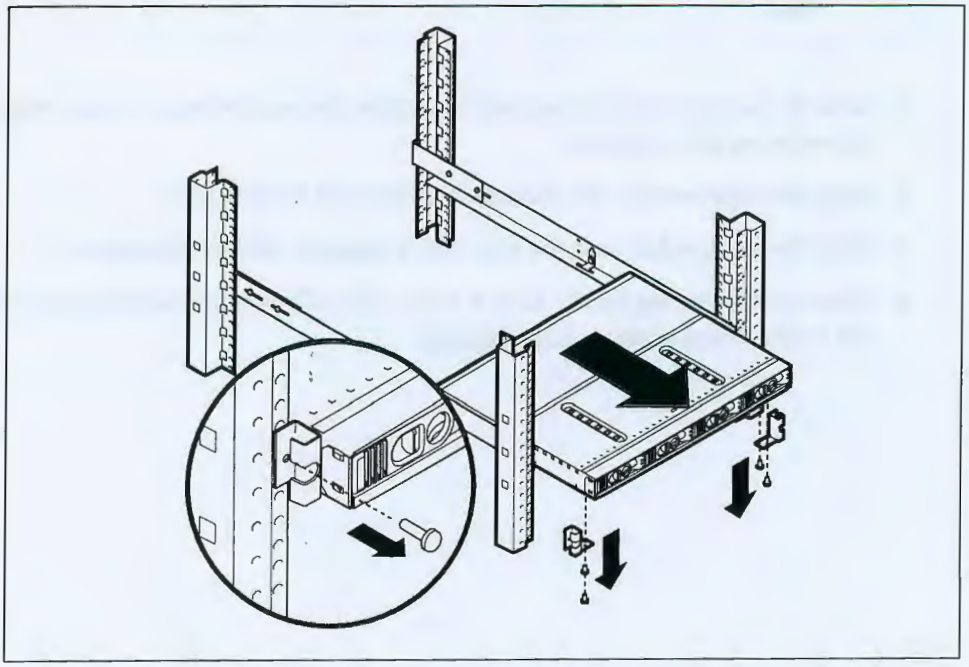
CAUTION **Some data paths may be slot-dependent. Be sure to note the slot from which the disk module is removed so it can be installed in the same slot in the replacement disk system.**

Reverse the installation instructions enclosed with the rackmount kit for your cabinet:

- A5679A for Hewlett-Packard Rack Systems/E for Enterprise Systems
- A5680A for all other Hewlett-Packard rack systems for Enterprise Systems purchased before November 1998.
- A6532A for Hewlett-Packard Rack Systems/E for Commercial Systems
- A6533A for all other Hewlett-Packard rack systems for Commerial Systems purchased before November 1998.

If your disk system is a factory-integrated unit, see the figure below for removal instructions.

FIGURE 12 Removing the Disk System



If you are returning a desktop disk system, be sure to remove and store the plastic Desktop Disk System Cover for use on the replacement disk system.

RQS nº 03/2005 - CN.
CPMI - CORREIOS
Fls. Nº 722
Doc: 3696

E C T 8846 Paula A C

2 Prepare the software environment to remove the drive.

See your operating system documentation for instructions and procedures required to remove a disk module. It may be necessary to unmount file systems associated with the disk drives installed in the disk system.

3 Unlatch the disk module handle and remove the disk module.

Squeeze the latch to unlock the disk module. Put a finger behind the latch and pull the disk module out until it disengages with the backplane. Leave it in its slot for two to three minutes to allow the disk drive to spin down before removing the disk module from the enclosure

If you are going to replace the disk module immediately, refer to "Replace a Disk Module" below.

If you are not going to replace the disk module immediately insert a filler panel into the open slot to assure the required cooling if you are not returning the disk system.

Replace a Disk Module

> **Note** The disk system supports the 18 and 36 GB disk capacity. It supports these capacities in 10,000 RPM disk modules only at this time.

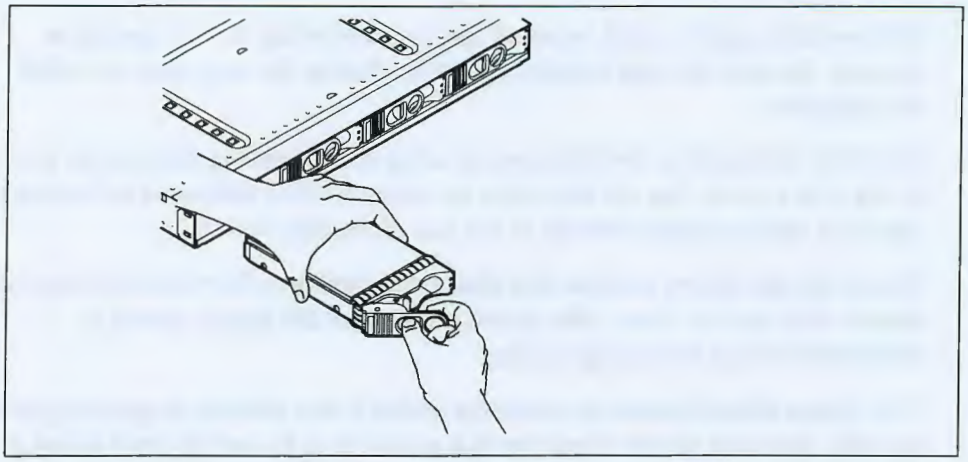
1 Refer to your operating system documentation for requirements and procedures for replacing disk modules.

2 Align the replacement disk module with the disk module slot.

3 Slide the disk module into the slot until it engages with the backplane.

4 Press on the locking handle until it locks. You will hear an audible click when the locking mechanism is fully engaged.

FIGURE 11 Installing a disk module



Configure the new Disk Module

Configure a New Disk Module within Your Application

CAUTION **These procedures should be performed only by qualified system administrator. Performing hot-plug operations on an active disk drive can result in data loss or corruption.**

Remove and Replace A Disk Module

Removing a Disk Module

CAUTION **If the disk system is running and a disk module slot does not contain a disk drive or filler panel, the disk system will not cool properly and may overheat. If you are not replacing the disk module immediately, a filler panel must be installed to maintain proper cooling.**
Ensure that you have a replacement disk or filler panel before removing the disk module from the disk system unless you are returning a defective disk system.

1 Ensure there is no activity on the drives.

If the Disk Drive LED for that disk module is flashing green, the disk drive is active. When the Disk Drive LED off, the disk module is either idle or completely off (see Table 1 on page 9). In this state, it is safe to remove the disk module.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 723
3698
Doc.

E C T
8818 Paula
C P L - A C

Adding Disk Modules

Disk modules can be added, removed, and replaced while the disk system is running. Because the disk modules can be handled in this way, they are called hot-pluggable.

The SCSI addresses for the disks are set using the addressing switches on the back of the disk system. You can determine the assigned SCSI addresses by looking at the SCSI address switch settings at the rear of the disk system.

If your storage system contains less than 4 disk modules, the remaining empty slots require filler panels. These filler panels ensure that the proper cooling is maintained within the storage system.

The system administration procedure for adding a disk modules is operating system specific. You must decide where the disk module is to be installed and install it. Then the operating system has to be configured to recognize the new disk drive.

> **Note** The disk system supports the 18 and 36 GB disk capacity points. It supports these capacities in 10,000 RPM disk modules only at this time.

Add a Disk Module

1. Select an available slot for the new disk module. Note the slot chosen for application configuration.
2. Remove the disk module filler panel. Store the filler panel for future use.
3. Hold the locking handle open on the disk drive. Push the locking lever to the left to release the latch.
4. Slide the disk into the appropriate slot.
5. Gently push the drive until the locking mechanism engages. When the disk modules is completely installed, an audible click can be heard.
6. Close the locking handle completely, using gentle downward pressure.

ECT - CPL - AC 8879 fls

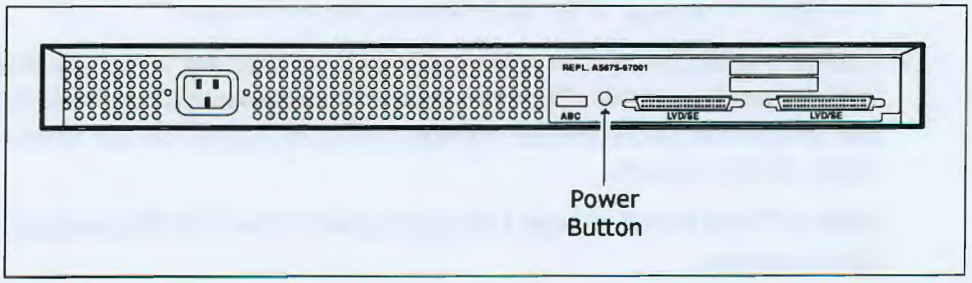
Power Off the Disk System

1. Back up all data if the disk system is still operational.
2. Ensure that no data on disk modules within the disk system is being accessed.
3. Unmount any file systems associated with the disk system that is going to be powered off. Refer to the system administration manual for your host system's operating system for the correct procedure for unmounting a file system or stopping access to the disk modules within the disk system.

> **Note** If your host system's boot or root disk drive resides in the disk system, the host system must be brought down before the power to the disk system can be turned off. See your host system's system administrator's manual for the correct procedures.

4. Turn the disk system off by pressing the power button. See Figure 10 (below) for the power button location.
5. Confirm that the storage disk system System Power LED is off. See Figure 2 on page 9
6. Disconnect the power cable from the power connector at the rear of the disk system.

FIGURE 10 Power Button Location



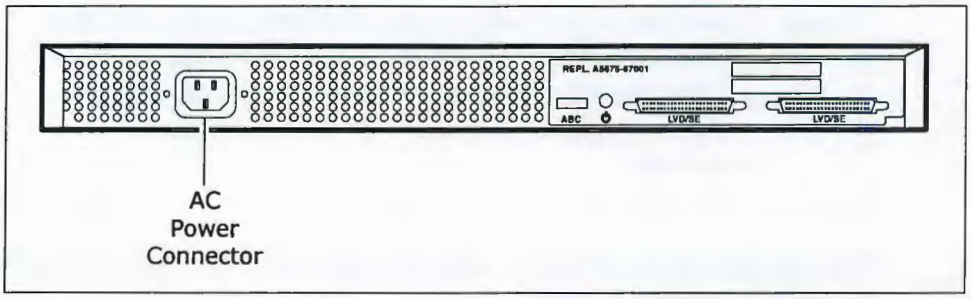
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 724
Doc.

E C T
CPL - AC

Connecting the Power Cable

CAUTION **Ensure that the connection of multiple units to the supply circuit does not overload the supply overcurrent protection or the supply wiring. Refer to the storage electrical ratings when determining the correct branch circuit rating for your installation. See Table 3 on page 12**

FIGURE 9 AC Power Connector Location



Powering On and Off

Power On the Disk System

1 Press the power button and release it. The power button will stay in a depressed position, indicating that the power is on

See Figure 10 on page 18 for the location of the power button.

2 Confirm that the disk system is running properly by checking the system power LED and the disk module LEDs at the front of your disk system. A system reboot may be necessary to assure that the host system recognizes the disk drives within the disk system.

Refer to "Front Panel" on page 3 for explanations of the LED functions and their meanings.

ECT - CPL - AC

4 Determine if this disk system is at the beginning or end of the SCSI bus.

- If the disk system is at the end of the SCSI bus (you are not going to daisy-chain another device off this one), install the appropriate terminator (part number 5183-2657) on the available SCSI port and go to "Connecting the Power Cable" (see Figure 9 on page 17).
- If the disk system is at the beginning or middle of the SCSI bus (you are going to daisy-chain another device off this one), consider the following:

  No more than 3 of these disk systems can be daisy-chained together.

  Ensure that the SCSI IDs assigned for the disk drives in the second disk system or other peripheral are not already assigned to another device on the SCSI bus. Refer to "Setting the SCSI IDs for the Disk Drives" (see Figure 7 on page 14 for the SCSI IDs assigned for each SCSI switch setting).

  If you connected the SCSI cable to the on-board UltraSCSI port on the host system, verify that the SCSI IDs assigned to the disk drives in the second disk system or additional peripherals are not already assigned to any other peripherals installed in the host system.

  The overall SCSI bus length cannot exceed 12 meters. The SCSI bus length for the disk system internal cables is 1.1 meters. If another type of peripheral is being connected on this SCSI bus, refer to that peripheral's documentation for its internal SCSI cable length.

5 Connect one end of an ultra SCSI cable (get it from the shipping box) to the available SCSI port on the rear of the first disk system on the SCSI bus.

6 Connect the other end of the ultrascsi cable to the SCSI IN port on the rear of the second disk system on the SCSI bus.

7 Repeat Steps 3, 5, and 6 for the last disk system on the SCSI bus if three disk systems are being installed. Keep in mind the maximum bus length (12 meters).

8 Install a terminator if the device is the last one on the bus. For supported terminators, see Table 10 on page 33 or Table 12 on page 34.

Note The disk system, when connected at the end of a SCSI bus, requires a terminator. Refer to the documentation that came with your wide SCSI device to determine if it needs a terminator or not. Narrow SCSI devices at the end of a daisy-chain always require a terminator.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 725
3698
Doc.

ECT 8883 Lausa CPL - AC

Keep in mind that the host bus adapter should have the highest SCSI address priority. See Table 5 below.

TABLE 5 SCSI Address Priority

SCSI ID	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
Priority	Highest															Lowest

Installing the Disk System

See the installation instructions enclosed with your rackmount kit.

Connect the SCSI Cables

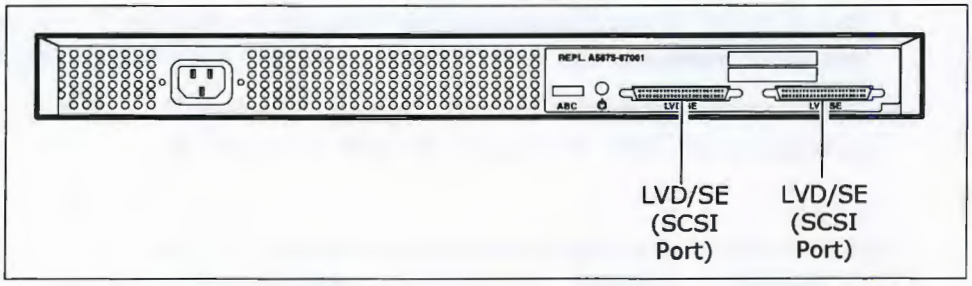
1 Make sure that the host system has been powered down.

2 Connect one end of an ultra SCSI cable (get it from the shipping box) to the host system. To acheive Ultra 3 SCSI speeds, the host bus adapter, the SCSI cables, and the disks must be able to transmit data at UltraSCSI 3 speeds. For the SCSI port location on your host system, refer to your host system's documentation.

You may connect non-Ultra 3 SCSI cables to the disk system, but the data transmission rates will be lower.

3 Connect the other end of the SCSI cable to one of the LVD/SE ports on the rear of the disk system.

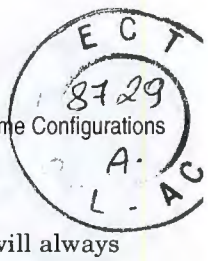
FIGURE 8 SCSI Port Locations



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 726
Doc. 3698

ECT
8128
CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 727
Doc. 3691



b. An input power source supplied from a 3-pole plus protective earth (PE), 4-wire system will always be wired as 240 volts phase-to-phase, no neutral or common, plus a PE ground. Three phase input voltage (240VAC) to the equipment is connected phase-to-phase. Examples of 4 wire: 200-volt phase-to-phase, 208-volt phase-to-phase, 240-volt phase-to-phase
c. An input power source supplied from a 4-pole +PE, 5 wire system may be wired as either:

208VAC phase-to-phase voltage with a common, plus a PE ground. Three phase input voltage (208VAC) to the equipment is connected phase-to-phase. The common is *not* connected to the PDCA neutral terminal.

415VAC phase-to-phase voltage with a neutral return, plus a PE ground. Three phase input voltage (230-240VAC) to the equipment is connected phase-to-neutral. The neutral is connected to the PDCA neutral terminal. Examples of 5 wire: 208-volt phase-to-phase, 380-volt phase-to-phase, 415-volt phase-to-phase

ECT
8732
A.
CPL - AC

Superdome LAN Interconnect Diagram

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 729
Doc.

Table D-1 LAN Information (Continued)

LAN Port:	Hostname (GSP Network Name)	IP Address	Subnet Mask	Gateway Address
Partition 5 (Net Interface 1)				
Partition 5 (Net Interface 2)				
Partition 5 (Net Interface 3)				

a. Superdome
b. Support Management Station

There are two columns of power numbers (Watts). The Power Breaker column shows the power used to size the wall breaker at the installation site. The Typical Power column shows typical power. Typical power numbers are for PA8600 systems and may be used to assess average utility cost of cooling and electrical power. Expect these typical numbers to be about 18% less for PA8700 systems. Table E-1 also shows the recommended breaker sizes for 4-wire and 5-wire sources.

Table E-1 Typical Superdome Configurations

Cell Boards	Memory Per Cell Board	I/O Chassis Modules	Breaker Power[a]	Recommended 3-pole Breaker Size[a,b]	Recommended 4-pole Breaker Size[a,c]	Typical Power	Typical Cooling
Qty.	GBytes	Qty.	Watts	Amps (min.)	Amps (min.)	Watts	BTU/HR
8	16	4	10660	40	25	8460	28,850
8	16	2	9600	40	25	7780	26,530
8	8	4	9220	40	25	7340	25,030
8	8	2	8160	30	20	6660	22,710
8	4	4	8500	35	20	6780	23,120
8	4	2	7440	30	20	6100	20,800
6	16	4	9040	35	20	7140	24,350
6	16	2	7980	30	20	6460	22,030
6	8	4	7960	30	20	6300	21,480
6	8	2	6900	30	20	5620	19,160
6	4	4	7420	30	20	5880	20,050
6	4	2	6360	30	20	5200	17,730
4	16	4	7420	30	20	5820	19,850
4	16	2	6360	30	20	5140	17,530
4	8	4	6700	30	20	5260	17,940
4	8	2	5640	25	20	4580	15,620
4	4	4	6340	30	20	4980	16,980
4	4	2	5280	25	20	4300	14,660
2	16	2	4740	20	20	3820	13,030
2	8	2	4380	20	20	3540	12,070
2	4	2	4200	20	20	3400	11,600

a. These numbers are valid only for the specific configurations shown. Any upgrades may require a change to the breaker size. A 5-wire source utilizes a 4 pole breaker and a 4-wire source utilizes a 3 pole breaker. *The PE (Protective Earth) ground wire is not switched.*

E Superdome Configurations

Table E-1 shows Superdome power requirements by configuration (i.e. number of cell boards, amount of memory per cell, and number of I/O chassis). This requirement applies to 32-way-capable systems with PA8600 or PA8700 processors.

- Console port on SMS
- Customer network interface on SMS (10/100 Base-T Port)
- Each network interface on each partition
- PC/Workstation console

Table D-1 LAN Information

LAN Port:	Hostname (GSP Network Name)	IP Address	Subnet Mask	Gateway Address
SD[a] GSP Private	Priv-nn (where *nn* is 01, 02, 03, ...)	192.168.2.1n (where *n* is 1, 2, 3, ...)	255.255.255.0	192.168.2.1n (where *n* is 1, 2, 3, ...)
SD Customer Port				
SMS[b] Customer Port (LAN 1, 10/100 BASE-T Port)				
SMS LAN Console				
SMS Private Port	PrivateM	192.168.2.10M (where M is 1, 2, 3, ...)	255.255.255.0	192.168.2.10M (where M is 1, 2, 3, ...)
PC/Workstation Console				
Partition 0 (Net Interface 1)				
Partition 0 (Net Interface 2)				
Partition 0 (Net Interface 3)				
Partition 1 (Net Interface 1)				
Partition 1 (Net Interface 2)				
Partition 1 (Net Interface 3)				
Partition 2 (Net Interface 1)				
Partition 2 (Net Interface 2)				
Partition 2 (Net Interface 3)				
Partition 3 (Net Interface 1)				
Partition 3 (Net Interface 2)				
Partition 3 (Net Interface 3)				
Partition 4 (Net Interface 1)				
Partition 4 (Net Interface 2)				
Partition 4 (Net Interface 3)				

ECT 18734 A. CPL

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 730
Doc. 3600

ECT
1 8135
A
CPL - A

D Superdome LAN Interconnect Diagram

Have the customer fill in Table D-1 on page 100 with LAN information. Use the following diagram to help correlate the LAN connection with the IP address.

You will need customer-supplied LAN information for:

- Customer port on GSP

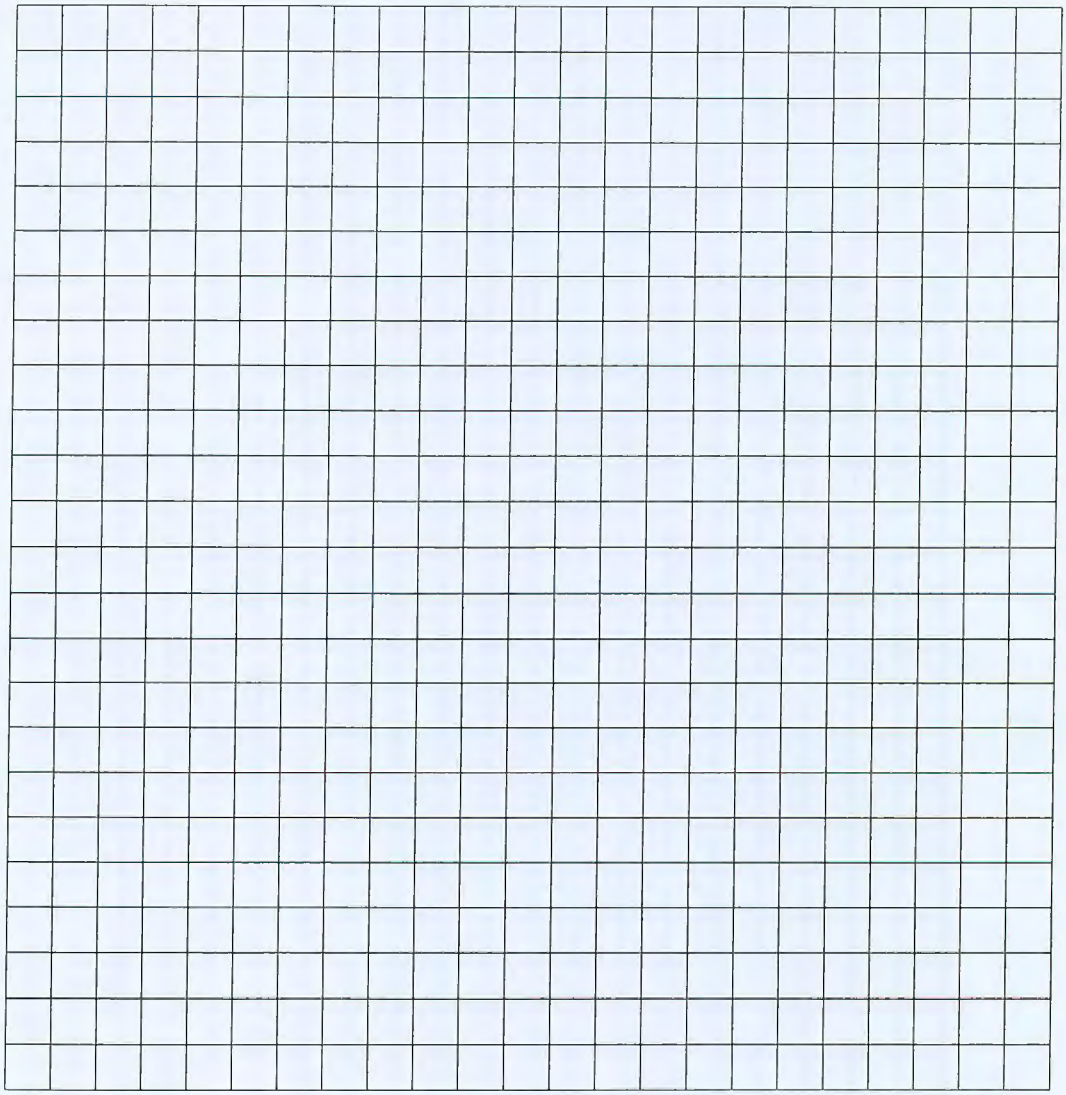
ECT
Templates
A. Computer Room Layout Plan
CPL - A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 731
Doc.

ECT
1813
A
CPL - AC

Computer Room Layout Plan

Scale: 1/4 inch = 1 foot



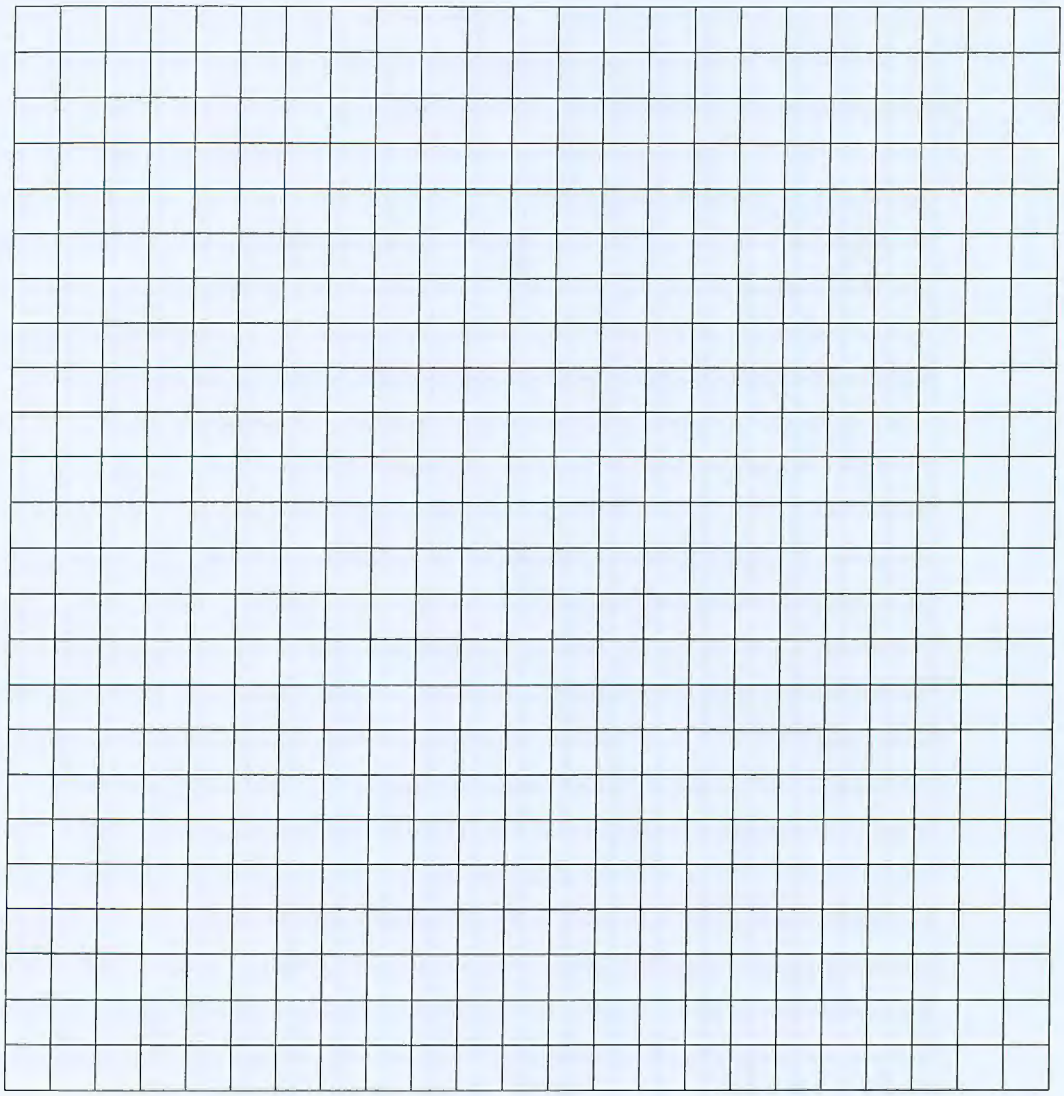
60SP016A
12/20/99

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 799
3698
Doc.

ECT
8740
A.
CPL - AC

Computer Room Layout Plan

Scale: 1/4 inch = 1 foot

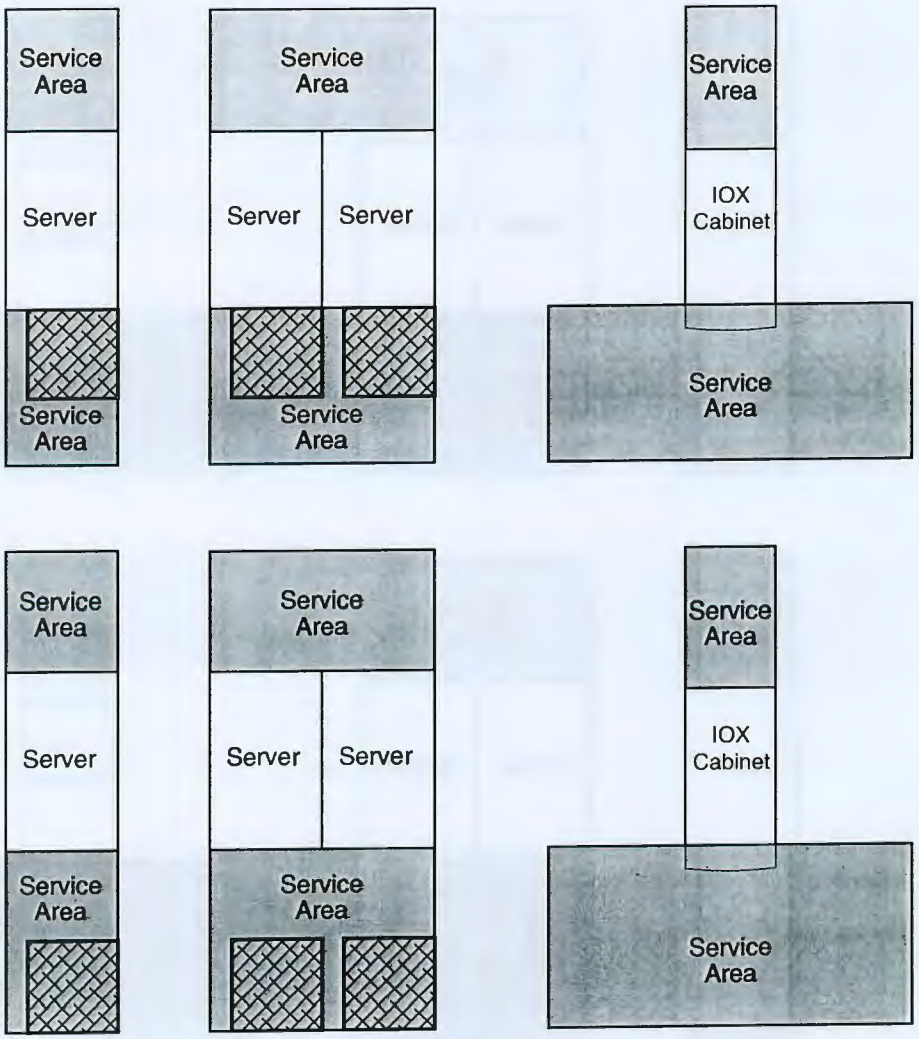


V25U067
10/2/98

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 733
Doc.

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

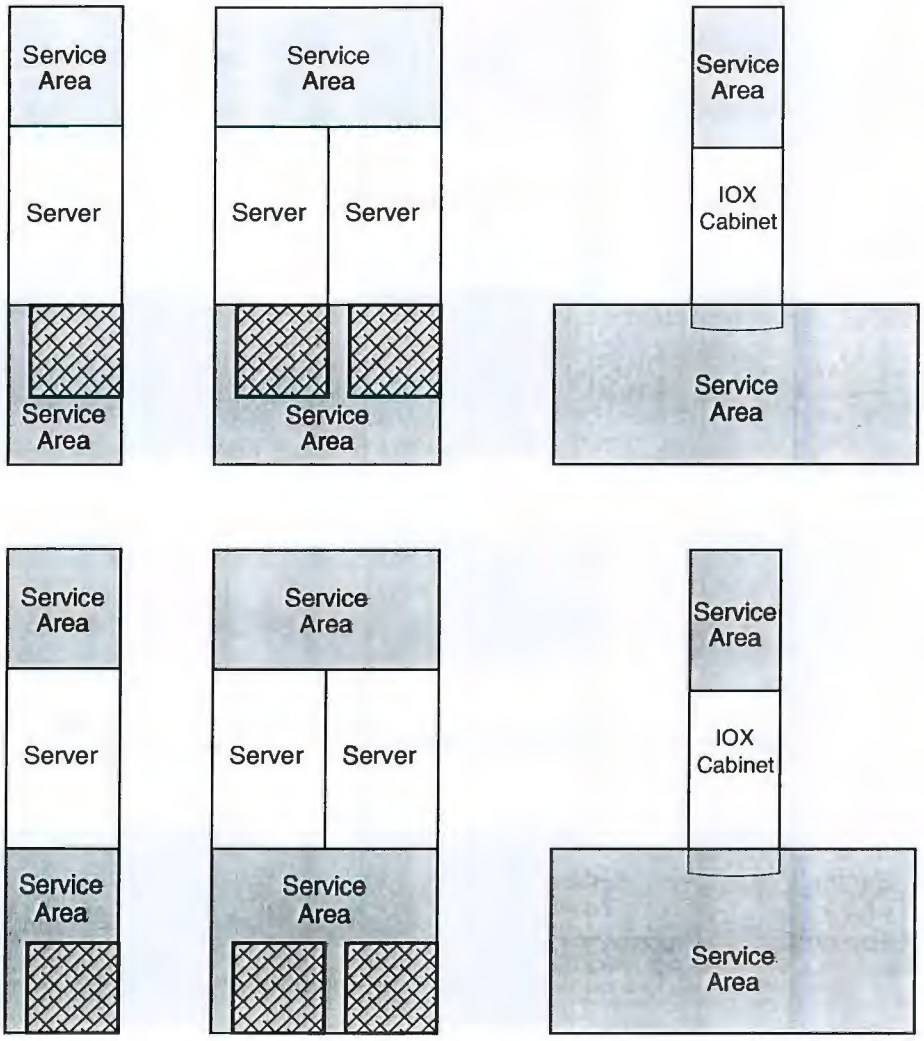
Scale: 1/4 inch = 1 foot



60SP017A
7/16/00

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

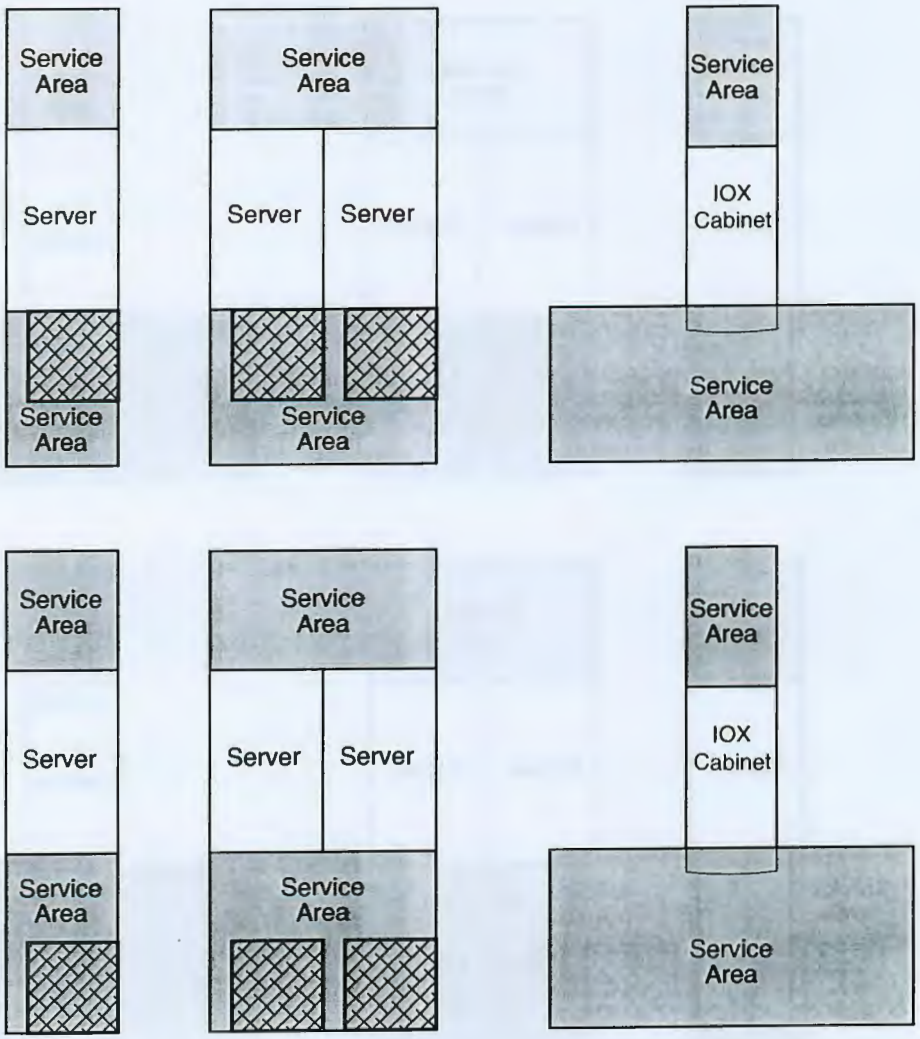
Scale: 1/4 inch = 1 foot



60SP017A
7/16/00

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

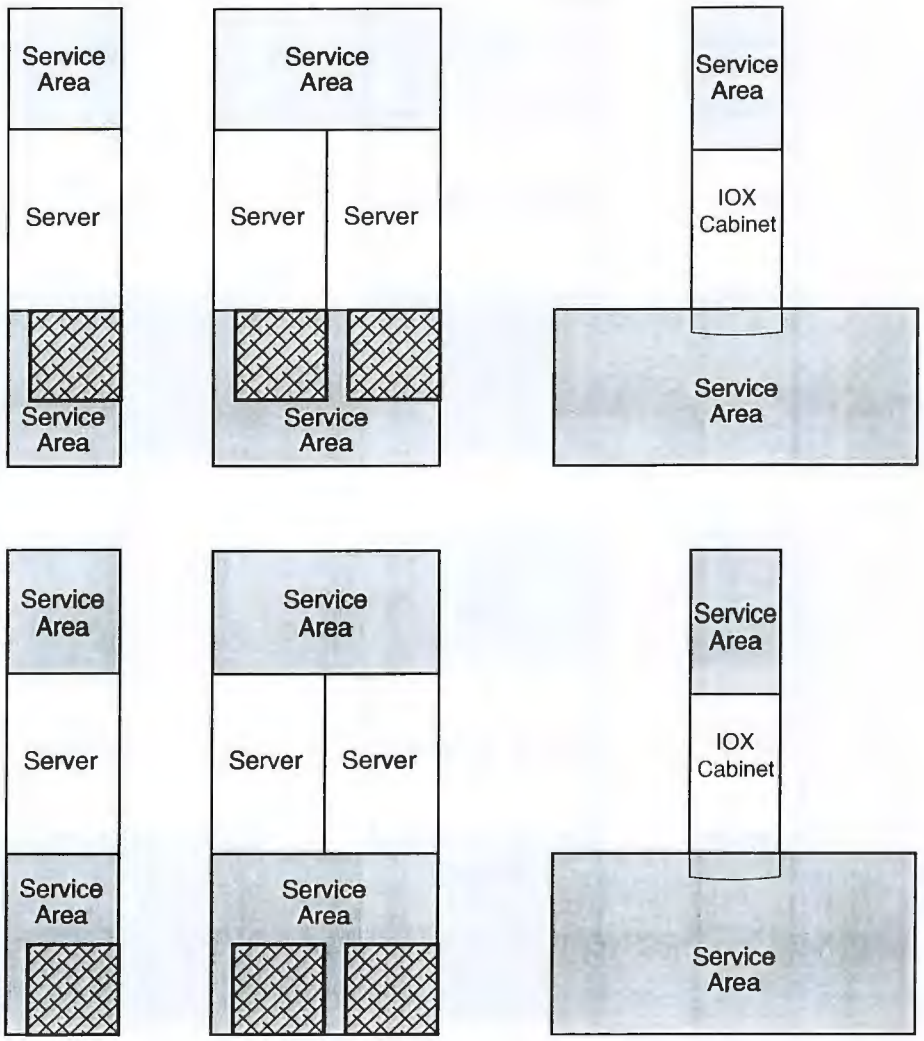
Scale: 1/4 inch = 1 foot



60SP017A
7/16/00

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

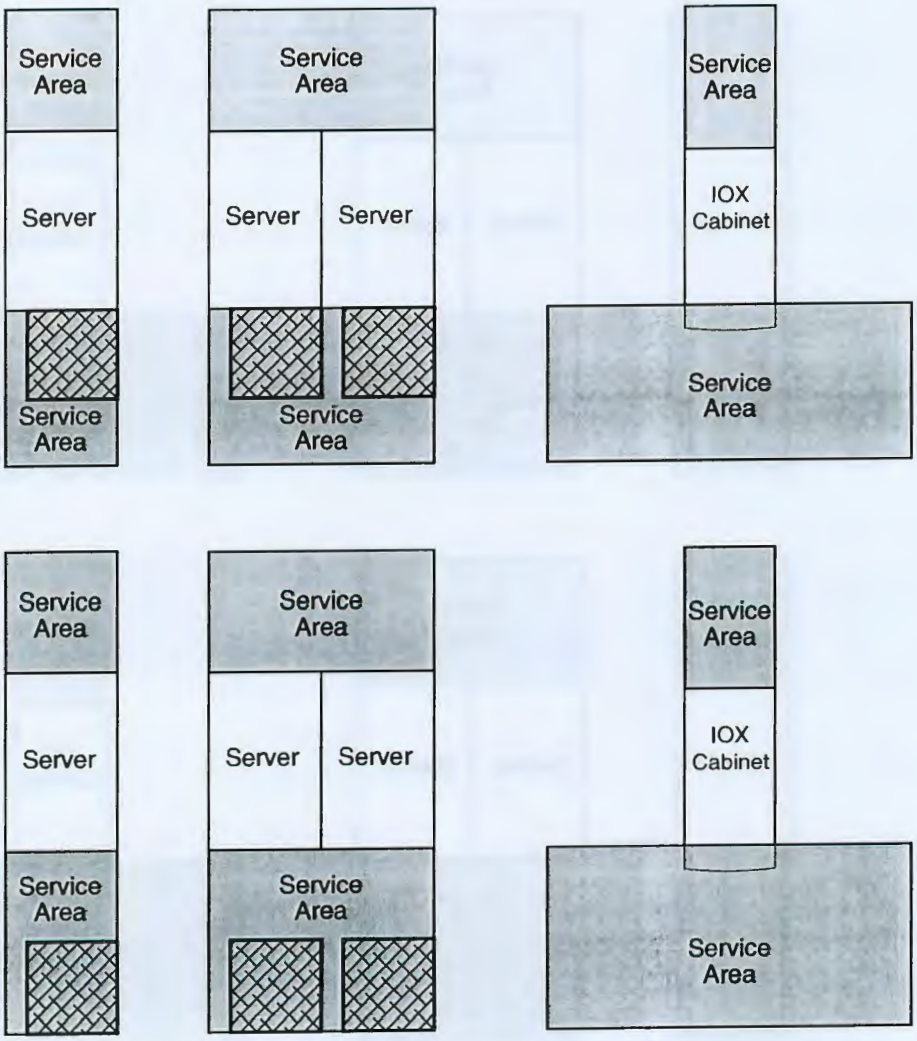
Scale: 1/4 inch = 1 foot



60SP017A
7/16/00

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot

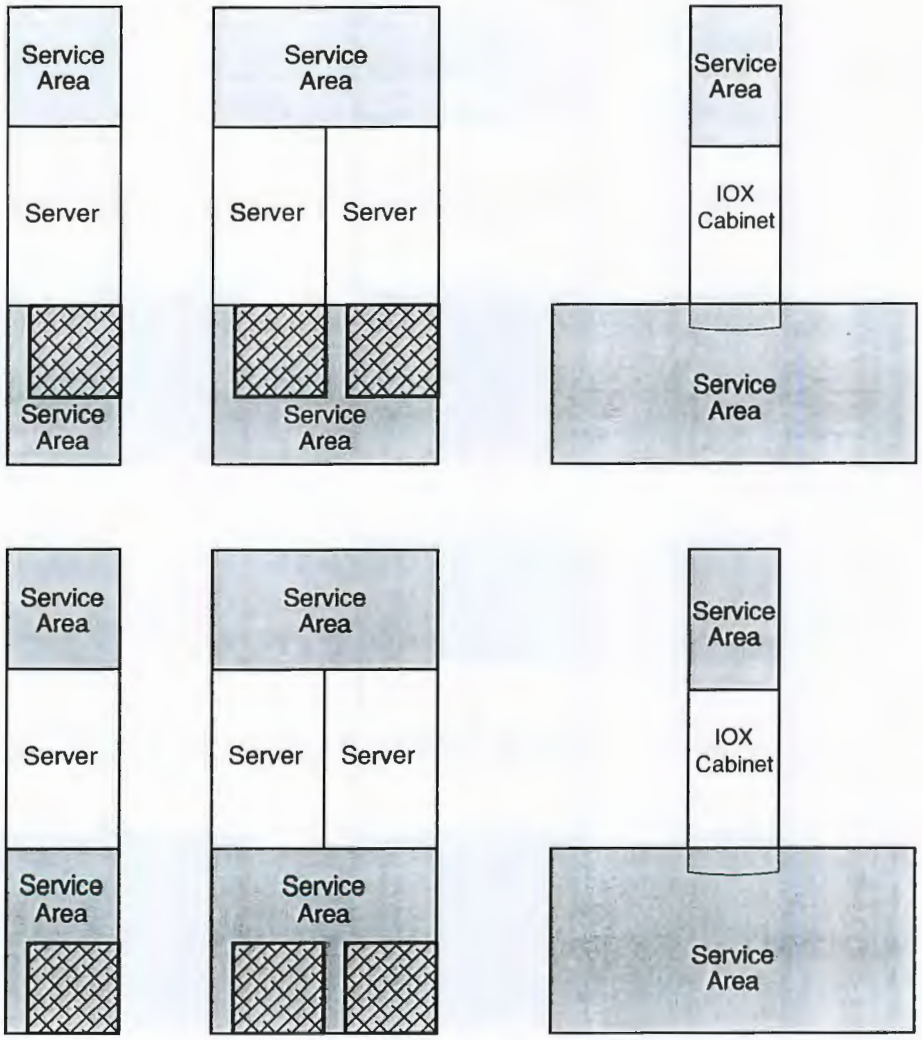


60SP017A
7/16/00

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 736
Doc.

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot



60SP017A
7/16/00

Computer Room Layout Plan

Use the following procedure to create a computer room layout plan:

Step 1. Remove several copies of the floor plan grid.

Step 2. Cut and join them together (as necessary) to create a scale model floor plan of your computer room.

Step 3. Remove a copy of each applicable equipment footprint template.

Step 4. Cut out each template selected in Step 3; then place it on the floor plan grid created in Step 2.

Step 5. Position pieces until the desired layout is obtained; then fasten the pieces to the grid. Mark locations of computer room doors, air-conditioning floor vents, utility outlets, and so on.

NOTE Attach a reduced copy of the completed floor plan to the site survey located in Chapter 4, "Pre-installation Survey." Hewlett-Packard field engineers use this floor plan during equipment installation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
737
Fls Nº
Doc 3600

Equipment Footprint Templates

Equipment footprint templates are drawn to the same scale as the floor plan grid (1/4 inch = 1 foot). These templates are provided to show basic equipment dimensions and space requirements for servicing.

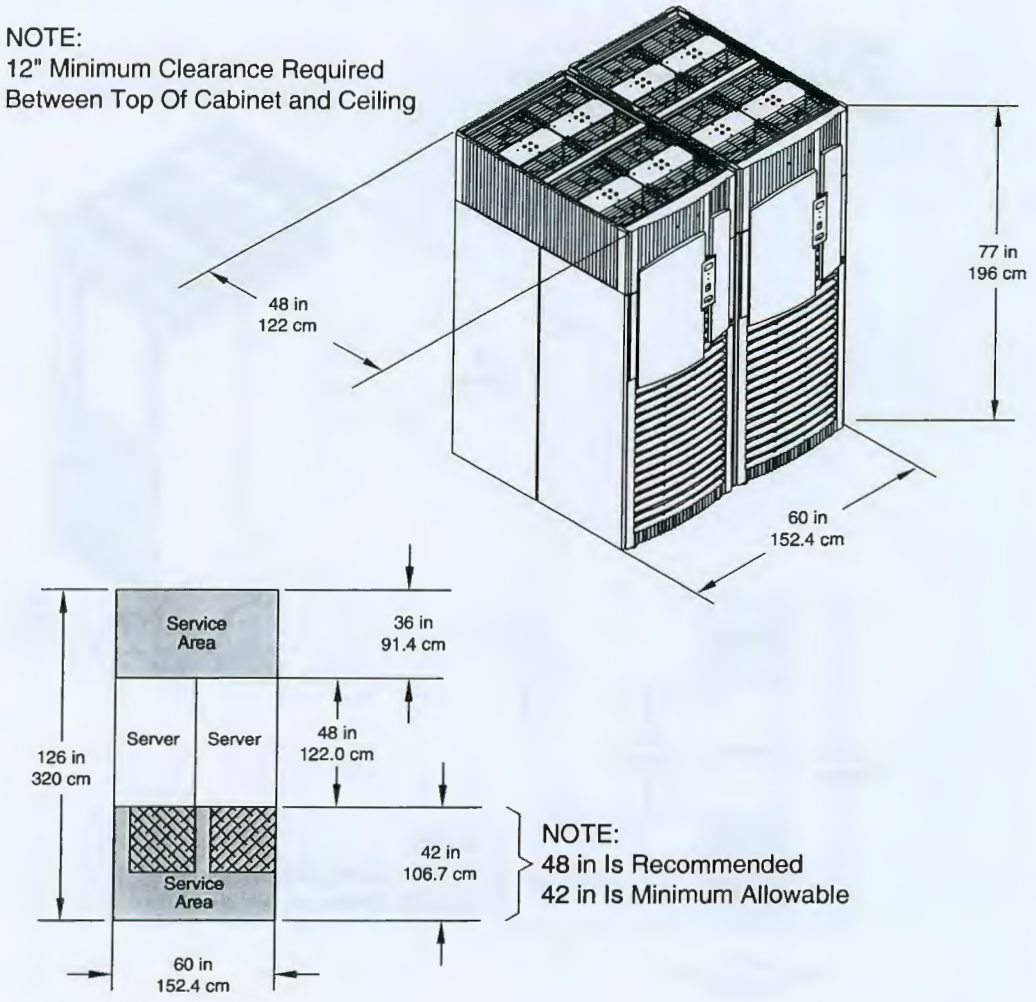
The service areas shown on the template drawings are lightly shaded.

The equipment templates should be used with the floor plan grid to define the location of the equipment that will be installed in your computer room.

NOTE Photocopying typically changes the scale of copied drawings. If any templates are copied, then all templates and floor plan grids must also be copied.

Templates
8150
A
C.P.L.

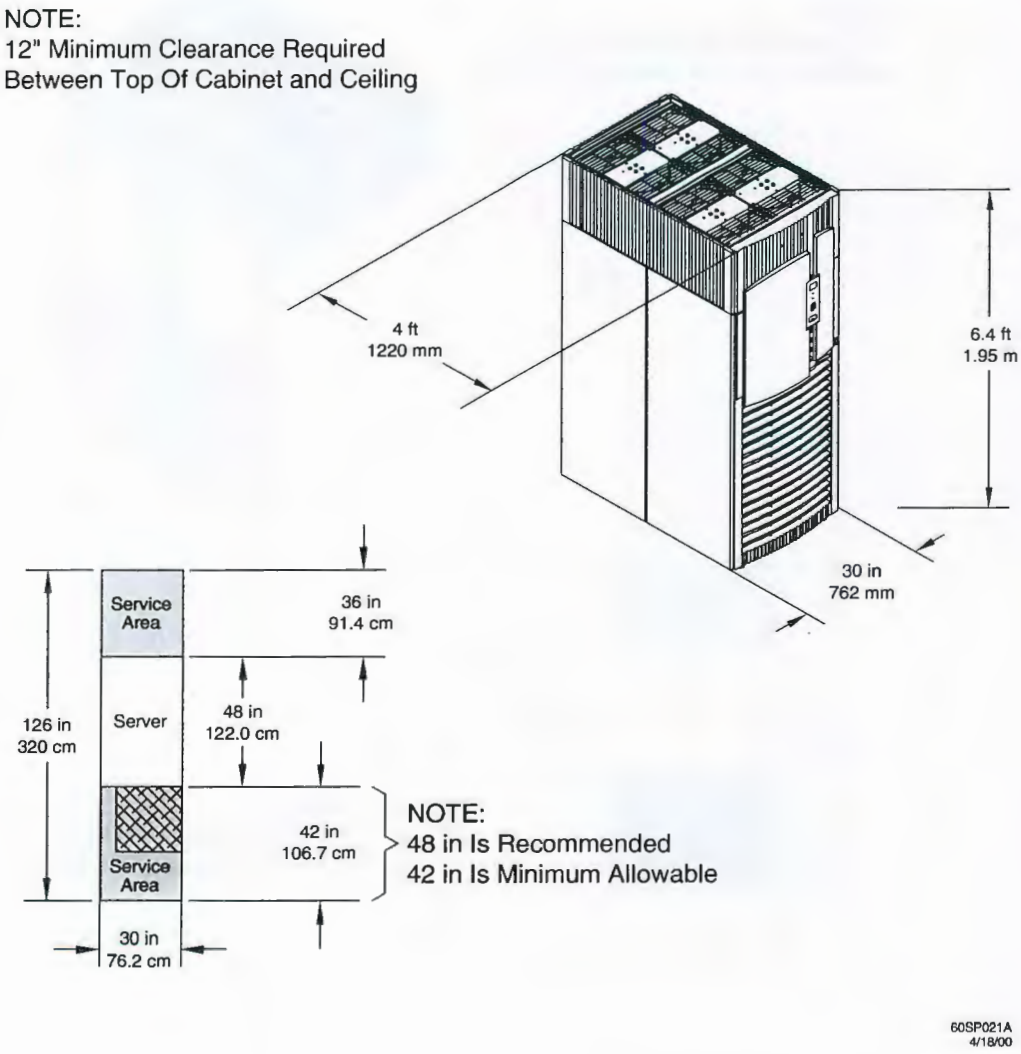
Figure C-3 Superdome 64 Way Space Requirements



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 738
Doc 3698

ECT
8751
Templates
A
CPL - AC

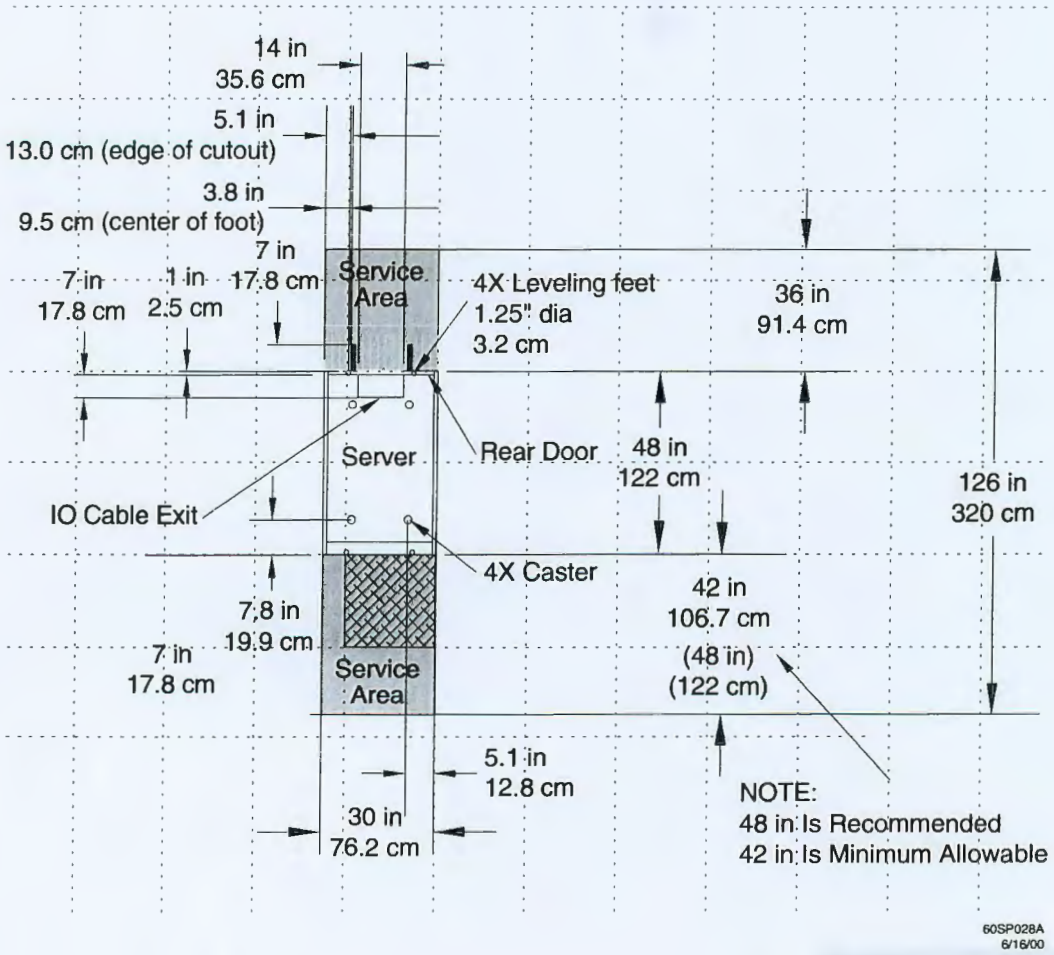
Figure C-2 Superdome 16 Way/Superdome 32 Way Space Requirements



ECT
8759
Templates
A.
CPL - AC

Figure C-3 on page 84 illustrates the overall dimensions required for a Superdome 64 Way system.

Figure C-1 Cable Cutouts and Caster Locations



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1790
Doc. 3698

C Templates

This appendix contains blank floor plan grids and equipment templates. Combine the necessary number of floor plan grid sheets to create a scaled version of the computer room floor plan.

Figure C-1 illustrates the locations required for the cable cutouts.

Figure C-2 on page 83 illustrates the overall dimensions required for a Superdome 32 Way system.

ECT 18754 A. CPL - C

- Refrigeration
  - 1 watt = .86 kcal/h
  - 1 watt = 3.413 Btu/h
  - 1 watt = 2.843-4 tons
  - 1 ton = 200 Btu/min
  - 1 ton = 12,000 Btu/h
  - 1 ton = 3,517.2 W
- Metric equivalents
  - 1 centimeter = 0.3937 in
  - 1 meter = 3.28 ft
  - 1 meter = 1.09 yds
  - 1 in. = 2.54 cm
  - 1 ft = 0.305 m
  - 1 CFM = 1.7m3/h
- kVA conversions, three ø

  $kVA = V \times A \times \sqrt{3} / 1000$
- kVA conversion, single ø

  $kVA = V \times A / 1000$

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 740
Doc. 3698

B Conversion Factors

The conversion factors provided in this appendix are intended to ease data calculation for systems that do not conform specifically to the configurations listed in this Site Preparation Guide.

Listed below are the conversion factors used in this document, as well as additional conversion factors that may be helpful in determining those factors required for site planning.

ECT
18756
A
CPL - AFC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 741
Doc.

System Weights A
Weight

Table A-2 Weight Summary (Continued)

Component	Quantity	Multiply By	Weight (kg)
PDCA		26.00lbs (23.59)	lbs
Bulk Power Supply (BPS)		23.00 lbs (11.81)	lbs
		Total weight	lbs

a. The listed weight for a chassis includes the weight of all components not listed in Table A-2.

Weight

To determine overall weight, follow the examples in Table A-1, then complete the entries in Table A-2.

Table A-1 Example Weight Summary

Component	Quantity	Multiply By	Weight (kg)
Chassis[a]	1	745.17 lbs (338.10)	745.17 lbs (338.10)
Cell Boards	4	41.00 lbs (18.60)	164.00 lbs (74.40)
DIMMs	128	.2 lbs (.09)	25.60 (11.60)
I/O Cardcages	4	36.5 lbs (16.56)	146 lbs (66.24)
I/O Cards	12	.45 lbs (.225)	5.4 lbs (2.45)
PDCA	2	26.00lbs (23.59)	104.00 lbs (47.18)
Bulk Power Supply (BPS)	6	23.00 lbs (11.81)	138.00 lbs (62.64)
		Total weight	1328.17lbs (517.35)

a. The listed weight for a chassis includes the weight of all components not listed in Table A-1.

Table A-2 Weight Summary

Component	Quantity	Multiply By	Weight (kg)
Chassis[a]		745.17 lbs (338.10)	745.17 lbs (338.10)
Cell Boards		41.00 lbs (18.60)	lbs
DIMMs		.2 lbs (.09)	lbs
I/O Cardcages		36.5 lbs (16.56)	lbs
I/O Cards		.45 lbs (.225)	lbs

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 449
3698
Doc.

ECT
CPL
Pre-Installation Survey
Delivery Survey

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 443
Doc. 3698

Figure 4-2 Delivery Survey (Part 2)

ELEVATOR

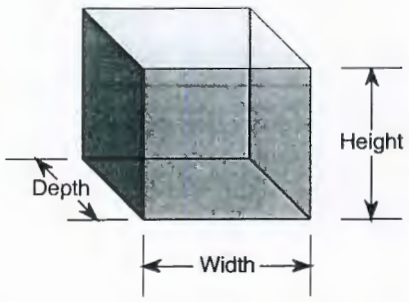
Fill in the following information if an elevator is required to move equipment.

Capacity (lb or kg) _____

Depth _____

Height _____

Width _____



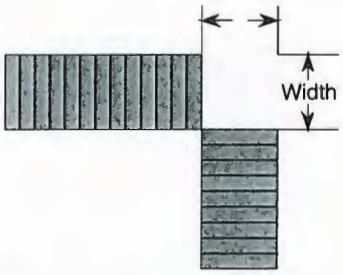
STAIRS

Please list number of flights and stairway dimensions.

Number of flights _____

Width _____

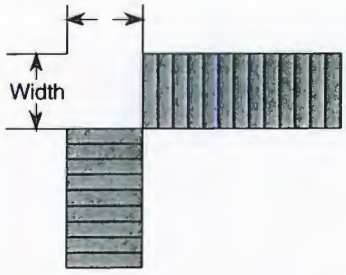
Width _____



Number of flights _____

Width _____

Width _____



60SP019A
11/24/99

Figure 4-1 Delivery Survey (Part 1)

DELIVERY CHECKLIST

DOCK DELIVERY

Is dock large enough for a semitrailer? Yes _____ No _____

Circle the location of the dock and give street name if different than address.

North

West East

South

STREET DELIVERY

Circle the location of access door and list street name if different than address.

North

West East

South

List height _____ and width _____ of access door.

List special permits (if required) for street delivery.

Permit type: Agency obtained from:

_____ _____

_____ _____

60SP018A
12/7/99

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 744
Doc

Delivery Survey

The delivery survey form shown in Figure 4-1 on page 72 and Figure 4-2 on page 73 lists delivery or installation requirements. If any of the items on the list apply, enter the appropriate information in the areas provided on the form.

Special instructions or recommendations should be entered on the Special Instructions or Recommendations form. Following are examples of special instructions or issues:

- Packaging restrictions at the facility, such as size and weight limitations
- Special delivery procedures
- Special equipment required for installation, such as tracking or hoists
- What time the facility is available for installation (after the equipment is unloaded)
- Special security requirements applicable to the facility, such as security clearance

ECT
8764
CPL
Pre-Installation Survey
Site Inspection

Table 4-2 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment or date				Comment or Date
26.	Are there any equipment servicing hazards (loose ground wires, poor lighting, etc.)?			
Cooling				
No.	Area or condition	Yes	No	
27.	Can cooling be maintained between 68° and 86° (20° and 30° C)?			
28.	Can temperature changes be held to 9° (5 ° C) per hour?			
29.	Can humidity level be maintained between 40% and 55%?			
30.	Are air conditioning filters installed and clean?			
Storage				
No.	Area or condition	Yes	No	
31.	Are cabinets available for tape and disc media?			
32.	Is shelving available for documentation?			
Training				
No.	Area or Condition			
33	Are personnel enrolled in the System Administrator's Course?			
34	Is on-site training required?			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 645
Doc. 3698

Table 4-2 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment or date				Comment or Date
11.	Are floor tiles in good condition and properly braced?			
12.	Metallic particulate test required.			
Power and lighting				
No.	Area or condition	Yes	No	
13.	Are lighting levels adequate for maintenance?			
14.	Are there ac outlets available for servicing needs? (i.e. vacuuming)			
15.	Does the input voltage correspond to equipment specifications?			
15A	Is dual source power used? If so, identify type(s) and evaluate grounding.			
16	Does the input frequency correspond to equipment specifications?			
17.	Are lightning arrestors installed inside the building?			
18.	Is power conditioning equipment installed?			
19.	Is there a dedicated branch circuit for equipment?			
20.	Is the dedicated branch circuit less than 250 feet (72.5 meters)?			
21.	Are the input circuit breakers adequate for equipment loads?			
Safety				
No.	Area or condition	Yes	No	
22.	Is there an emergency power shut-off switch?			
23.	Is there a telephone available for emergency purposes?			
24.	Is there a fire protection system in the computer room?			
25.	Is antistatic flooring installed?			

NOTE To ensure compliance with item 10 of Table 4-2, provide a copy of Appendix D to the customer to use a worksheet to identify required names and addresses for the LAN.

Table 4-2 Site Inspection Checklist

Please check either Yes or No. If No, include comment or date				Comment or Date
Computer room				
No.	Area or condition	Yes	No	
1.	Is there a completed floor plan?			
2.	Is there adequate space for maintenance needs? Front 42 in (106 cm) min., 48 in (121 cm) recommended. Rear 32 in (81 cm) min., 36 in (91cm) recommended			
3.	Is access to the site or computer room restricted?			
4.	Is the computer room structurally complete? Expected date of completion?			
5.	Is a raised floor installed and in good condition? What is the floor to ceiling height? [7.5 ft (228 cm) minimum]			
6.	Is the raised floor adequate for equipment loading?			
7.	Are there channels or cutouts for cable routing?			
8.	Is there a remote console telephone line available with an RJ11 jack?			
9.	Is a telephone line available?			
9a.	Is the customer aware of the iCOD email requirements? Each bootable partition requires a connection to the internet to send email to notify Hewlett-Packard that the customer has allocated additional CPUs beyond the amount initially purchased. Each bootable partition must be configured to perform this operation. For more details, go to http://superdome.hp.com and click on the iCOD link.			
10.	Are customer supplied peripheral and LAN cables available and of the proper type?			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1646
Doc. 3698

Site Inspection

Table 4-1 contains a sample of the Customer and Hewlett-Packard information required.

Table 4-2 contains a sample site inspection checklist.

IMPORTANT Ensure that the customer is aware of the iCOD email requirements. That is, each bootable partition requires a connection to the internet to send email to notify Hewlett-Packard that the customer has allocated additional CPUs beyond the amount initially purchased. Each bootable partition must be configured to perform this operation.

For more details, go to http://superdome.hp.com and click on the iCOD link.

NOTE Table 4-1 and Table 4-2 are provided as examples only. To ensure use of the current information specific to your site preparation, refer to the Site Readiness Review Section of the Deployment Manager's Handbook.

Table 4-1 Customer and Hewlett-Packard Information

Customer Information	
Name:	Phone No:
Street Address:	City or Town:
State or Province:	Country
Zip or postal code:	
Primary customer contact:	Phone No.:
Secondary customer contact:	Phone No.:
Traffic coordinator:	Phone No.:
Hewlett-Packard information	
Sales representative	Order No:
Representative making survey	Date:
Scheduled delivery date	

ECT 8168 A CPL 42

Typical Installation Schedule

The following schedule lists the sequence of events for a typical system installation:

- 60 days before installation
  - — Floor plan design completed and mailed to Hewlett-Packard
- 30 days before installation
  - — Primary power and air conditioning installation completed
  - — Telephone and data cables installed
  - — Fire protection equipment installed
  - — Major facility changes completed
  - — Special delivery requirements defined
  - — Site inspection survey completed
  - — Delivery survey completed
  - — Signed copy of the site inspection and delivery survey mailed to Hewlett-Packard
  - — Site inspection and pre-delivery coordination meeting arranged with a Hewlett-Packard representative to review the inspection checklist and arrange an installation schedule.
- 7 days before installation
  - — Final check made with a Hewlett-Packard customer engineer to resolve any last-minute problems

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 747
Doc. 3698

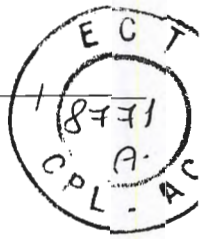
Pre-Installation Survey Content

The site pre-installation survey information is designed to identify problems that might occur before, during, or after the installation of the system. It contains the following items:

- Pre-installation checklists—Verify the customer site is ready for the equipment installation.
- Pre-installation survey information sheets—List customer name, address, and corresponding Hewlett-Packard sales personnel.
- Pre-installation survey information forms—List delivery information and special instructions.

- "Typical Installation Schedule" on page 66 describes the proposed schedule of installation events.
- "Site Inspection" on page 67 provides a sample pf the on-site inspection checklist.
- "Delivery Survey" on page 71 provides the delivery or installation requirement forms.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 640
Doc. 3698



4 Pre-Installation Survey

This chapter provides a site survey information packet consisting of an information form and checklists to be used to evaluate a computer facility. The checklists information sheets and information forms should be filled out by the customer and a Hewlett-Packard representative.

- "Pre-Installation Survey Content" on page 65 describes the contents of the site survey information packet.

ECTI 8772 A- 5 CPL -

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 144
Doc. 3698

- Access areas for power wiring and air conditioning filters
- Equipment cable routing

Copies of the floor plan grid are located in Appendix C.

Equipment Footprint Templates

Equipment footprint templates are provided in Appendix C to show basic equipment dimensions and space requirements for servicing. Be sure to use the appropriate templates for the equipment that is to be installed.

The service areas shown on the template drawings are lightly shaded.

Removable copies of the equipment footprint templates are located in Appendix C. They should be used with the floor plan grid to define the location of the equipment that will be installed in your computer room.

NOTE Photocopying typically changes the scale of drawings copied. If any templates are copied, then all templates and floor plan grids must also be copied.

ECT 8774 A CPL - AC

Space Requirements

This section contains information about space requirements for a Superdome server. This data should be used as the basic guideline for space plan developments. Other factors, such as airflow, lighting, and equipment space requirements, must also be considered.

Delivery Space Requirements

There should be enough clearance to move equipment safely from the receiving area to the computer room. Permanent obstructions, such as pillars or narrow doorways, can cause equipment damage.

Delivery plans should include the possible removal of walls or doors. The physical dimensions for applicable computers and peripheral equipment are summarized in Appendix A.

Operational Space Requirements

Other factors must be considered along with the basic equipment dimensions. Reduced airflow around equipment causes overheating, which can lead to equipment failure. Therefore, the location and orientation of air conditioning ducts, as well as airflow direction, are important. Obstructions to equipment intake or exhaust airflow must be eliminated.

The location of lighting fixtures and utility outlets affects servicing operations. Plan equipment layout to take advantage of lighting and utility outlets. Do not forget to include clearance for opening and closing equipment doors.

Clearance around and above the cabinets must be provided for proper cooling airflow through the equipment.

The service area space requirements, outlined in Appendix C, are minimum dimensions. If other equipment is located so that it exhausts heated air near the cooling air intakes of the computer system cabinets, larger space requirements are needed to keep ambient air intake to the computer system cabinets within the specified temperature and humidity ranges.

Space planning should also include the possible addition of equipment or other changes in space requirements. Equipment layout plans should also include provisions for the following:

- Channels or fixtures used for routing data cables and power cables
- Access to air conditioning ducts, filters, lighting, and electrical power hardware
- Power conditioning equipment
- Cabinets for cleaning materials
- Maintenance area and spare parts

Floor Plan Grid

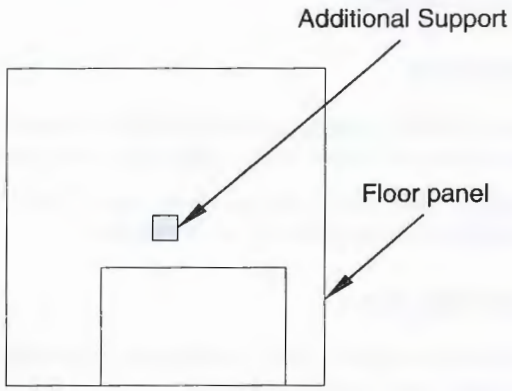
The floor plan grid is used to plan the location of equipment in the computer room. In addition to its use for planning, the floor plan grid should also be used when planning the locations of the following items:

- Air conditioning vents
- Lighting fixtures
- Utility outlets
- Doors

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 750
Doc.

In the event that the flooring is being replaced or a new floor is being installed, Tate Access Floors recommends its Series 1250 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels be used to support the Superdome installation.

Figure 3-1 Tate Series 800 Floor Bracing



NOTE If the specific floor being evaluated or considered is other than a Tate Series 800 floor, the specific floor manufacturer must be contacted to evaluate the floor being used.

Table 3-2 lists specifications for the Tate Access Floors Series 800 raised-floor system.

Table 3-2 Tate Series 800 Raised-Floor Tile Specifications

Item	Rating
Dead load	7 lb/ft 2 (34.2 kg/m2)
Live load	313 lb/ft 2 (1528.3 kg/m2)
Concentrated load[a]	1250 lb (567 kg)
Ultimate load	4000 lb (1814 kg) per panel
Rolling load	400 lb (181 kg)
Average Tile load	500 lb (227 kg)

a. With 0.08 in (0.2 cm) of span maximum deflection

Windows

Avoid housing computers in a room with windows. Sunlight entering a computer room may cause problems. Magnetic tape storage media is damaged if exposed to direct sunlight. Also, the heat generated by sunlight places an additional load on the cooling system.

Table 3-1 Floor-Loading Terms (Continued)

Term	Definition
Concentrated load	Load a floor panel can support on a 1-in2 (6.45 cm2) area at the panel's weakest point (typically the center of the panel), without the surface of the panel deflecting more than a predetermined amount.
Ultimate load	Maximum load (per floor panel) the floor system can support without failure. Failure expressed by floor panel(s) breaking or bending. Ultimate load is usually stated as load per floor panel.
Rolling load	Load a floor panel can support (without failure) when a wheel of specified diameter and width is rolled across the panel.
Average floor load	Computed by dividing total equipment weight by the area of its footprint. This value is expressed in lb/ft2 (kg/m2).

Average Floor Loading

The average floor load value, defined in Table 3-2, is not appropriate for addressing raised-floor ratings at the floor grid spacing level. However, it is useful for determining floor-loading at the building level, such as the area of solid floor or span of raised-floor tiles covered by the Superdome server footprint.

Typical Raised-Floor Site

This section contains an example of a computer room raised-floor system that is satisfactory for the installation of a Superdome server.

Based on specific information provided by Hewlett-Packard, Tate Access Floors has approved its Series 800 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels.

Due to the large amount of floor panel material that must be removed for the purpose of routing cables, this particular floor must be braced as shown in Figure 3-1.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc.

Facility Characteristics

This section contains information about facility characteristics that must be considered for the installation or operation of a Superdome server. Facility characteristics are:

- Floor loading
- Windows
- Altitude effects

Floor Loading

The computer room floor must be able to support the total weight of the installed computer system as well as the weight of the individual cabinets as they are moved into position.

Floor loading is usually not an issue in non-raised-floor installations. The information presented in this section is directed toward raised-floor installations.

NOTE Any floor system under consideration for a Superdome server installation should be verified by an appropriate floor system consultant.

Raised-Floor Loading

Raised-floor loading is a function of the manufacturer's load specification and the positioning of the equipment relative to the raised-floor grid. While Hewlett-Packard cannot assume responsibility for determining the suitability of a particular raised-floor system, information and illustrations are provided for the customer or local agencies to determine installation requirements.

The following guidelines are recommended:

- Because many raised-floor systems do not have grid stringers between floor stands, the lateral support for the floor stands depends on adjacent panels being in place. To avoid compromising this type of floor system while gaining under floor access, remove only one floor panel at a time.
- Larger floor grids (bigger panels) are generally rated for lighter loads.

CAUTION Do not install any raised-floor system until you have carefully examined it to verify that it is adequate to support the appropriate installation.

Floor-Loading Terms

Table 3-1 defines floor-loading terms.

Table 3-1 Floor-Loading Terms

Term	Definition
Dead load	Weight of the raised-panel floor system, including the understructure. Expressed in lb/ft2 (kg/m2).
Live load	Load the floor system can safely support. Expressed in lb/ft2 (kg/m2).

NOTE Refer to Appendix C for templates to aid in locating caster contact area and caster/leveling foot centers. Templates are also provided to locate required cutouts for cable routing.

RQS nº 03/2005 - CN
CPMi - CORREIOS
Fls. Nº
Doc.

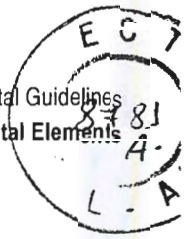
3 Facility Guidelines

This chapter describes facility characteristics and provides guidelines for preparing the computer room.

- "Facility Characteristics" on page 57 discusses architectural issues.
- "Space Requirements" on page 60 discusses the amount of floor space required by the components.

E C T
1 8780 A
CPL - AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 753
Doc. 3698



Static Protection Measures

Follow these precautions to minimize possible ESD-induced failures in the computer room:

- Install conductive flooring (conductive adhesive must be used when laying tiles).
- Use conductive wax (if waxed floors are necessary).
- Ensure that all equipment and flooring are properly grounded and are at the same ground potential.
- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) when handling circuit boards.
- Store spare electronic modules in antistatic containers.
- Maintain recommended humidity level and airflow rates in the computer room.

Acoustics

Computer equipment and air conditioning blowers cause computer rooms to be noisy. Ambient noise level in a computer room can be reduced as follows:

- Dropped ceiling—Cover with a commercial grade of fire-resistant, acoustic rated, fiberglass ceiling tile.
- Sound deadening—Cover the walls with curtains or other sound deadening material.
- Removable partitions—Use foam rubber models for most effectiveness.

Special precautions are necessary if the computer room is near a source of air pollution. Some air pollutants, especially hydrogen sulfide (H2S), are not only unpleasant but corrosive as well. Hydrogen sulfide damages wiring and delicate sound equipment. The use of activated charcoal filters reduces this form of air pollution.

Zinc Particulate Contamination

Metallic particulates can be especially harmful around electronic equipment. This type of contamination may enter the data center environment from a variety of sources, including but not limited to raised floor tiles, worn air conditioning parts, heating ducts, rotor brushes in vacuum cleaners or printer component wear. Because metallic particulates conduct electricity, they have an increased potential for creating short circuits in electronic equipment. This problem is exaggerated by the increasingly dense circuitry of electronic equipment.

Over time, very fine whiskers of pure metal can form on electroplated zinc, cadmium, or tin surfaces. If these whiskers are disturbed, they may break off and become airborne, possibly causing failures or operational interruptions. For over 50 years, the electronics industry has been aware of the relatively rare but possible threat posed by metallic particulate contamination. During recent years, a growing concern has developed in computer rooms where these conductive contaminants are formed on the bottom of some raised floor tiles.

Although this problem is relatively rare, it may be an issue within your computer room. Since metallic contamination can cause permanent or intermittent failures on your electronic equipment, Hewlett-Packard strongly recommends that your site be evaluated for metallic particulate contamination before installation of electronic equipment.

Electrostatic Discharge (ESD) Prevention

Static charges (voltage levels) occur when objects are separated or rubbed together. The voltage level of a static charge is determined by the following factors:

- Types of materials
- Relative humidity
- Rate of change or separation

Table 2-2 lists charge levels based on personnel activities and humidity levels.

Table 2-2 Effect of Humidity on ESD Charge Levels

Personnel Activity[a]	Humidity[b] and Charge Levels (volts)[c]			
	26%	32%	40%	50%
Walking across a linoleum floor	6,150	5,750	4,625	3,700
Walking across a carpeted floor	18,450	17,250	13,875	11,100
Getting up from a plastic chair	24,600	23,000	18,500	14,800

a. Source: B.A.Unger, Electrostatic Discharge Failures of Semiconductor Devices (Bell Laboratories,1981)
b. For the same relative humidity level, a high rate of airflow produces higher static charges than a low airflow rate.
c. Some data in this table has been extrapolated.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.
Doc.

E C T
8783
D L - A C

CAUTION Low humidity contributes to undesirably high levels of electrostatic charges. This increases the electrostatic discharge (ESD) voltage potential. ESD can cause component damage during servicing operations. Paper feed problems on high-speed printers are usually encountered in low-humidity environments.

Low humidity levels are often the result of the facility heating system and occur during the cold season. Most heating systems cause air to have a low humidity level, unless the system has a built-in humidifier.

Air Conditioning Ducts

Use separate computer room air conditioning duct work. If it is not separate from the rest of the building, it might be difficult to control cooling and air pressure levels. Duct work seals are important for maintaining a balanced air conditioning system and high static air pressure. Adequate cooling capacity means little if the direction and rate of air flow cannot be controlled because of poor duct sealing. Also, the ducts should not be exposed to warm air, or humidity levels may increase.

Dust and Pollution Control

Computer equipment can be adversely affected by dust and microscopic particles in the site environment.

Specifically, disk drives, tape drives, and some other mechanical devices can have bearing failures resulting from airborne abrasive particles. Dust may also blanket electronic components like printed circuit boards causing premature failure due to excess heat and/or humidity build up on the boards. Other failures to power supplies and other electronic components can be caused by metallically conductive particles. These metallic particles are conductive and can short circuit electronic components. Use every effort to ensure that the environment is as dust and particulant free as possible.

Smaller particles can pass though some filters and, over a period of time, possibly cause problems in mechanical parts. Small dust particles can be prevented from entering the computer room by maintaining its air conditioning system at a high static air pressure level.

Other sources of dust, metallic, conductive, abrasive, and/or microscopic particles can be present. Some sources of these particulants are:

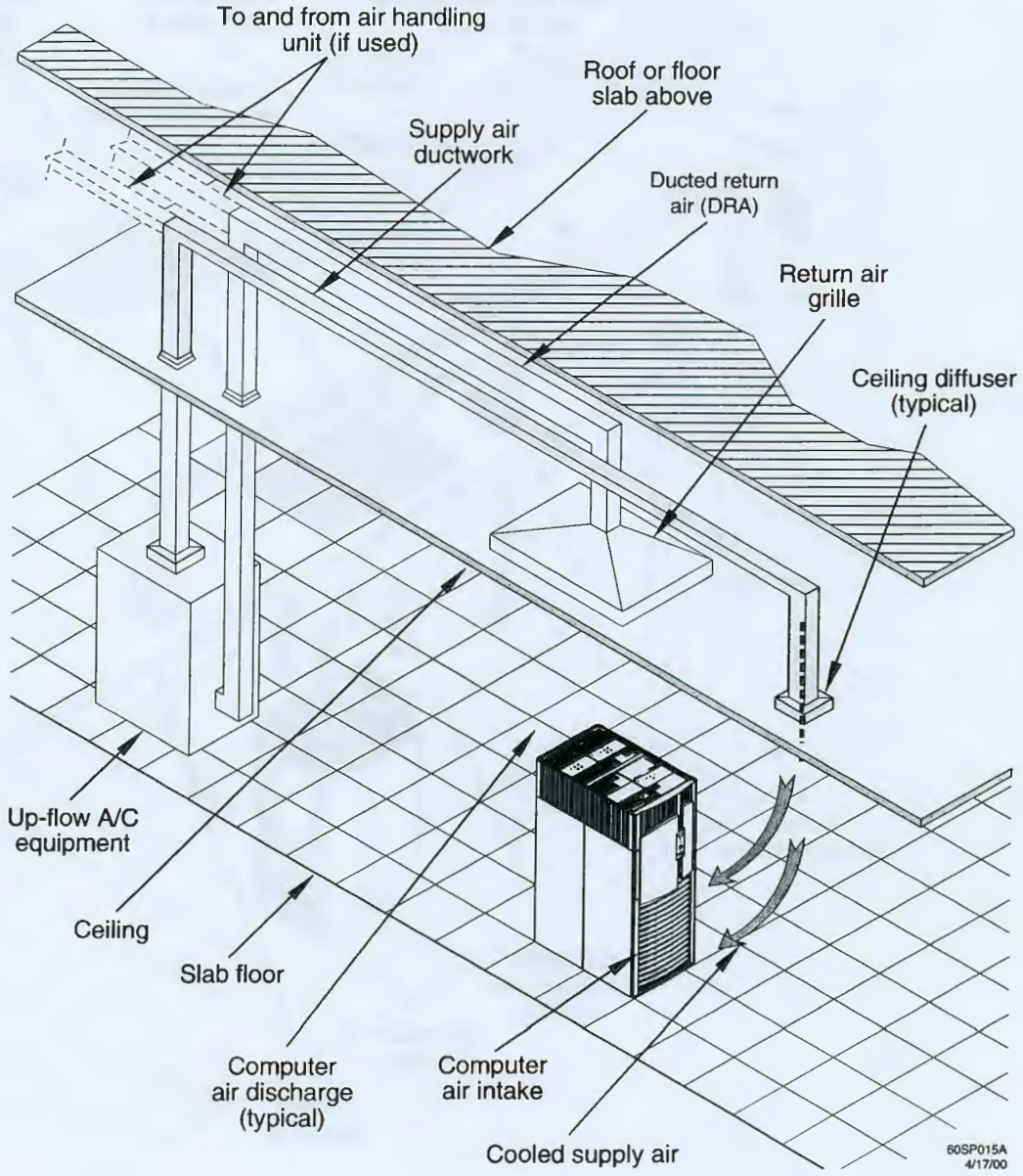
- Subfloor shedding
- Raised floor shedding
- Ceiling tile shedding

These pollutants are not always visible to the naked eye. A good check to determine their possible presence is to check the underside of the tiles. The tile should be shiny, galvanized, and free from rust.

The computer room should be kept clean. The following guidelines are recommended:

- Smoking—Establish a no-smoking policy. Cigarette smoke particles are eight times larger than the clearance between disk drive read/write heads and the disk surface.
- Printer—Locate printers and paper products in a separate room to eliminate paper particulate problems.
- Eating or drinking—Establish a no-eating or drinking policy. Spilled liquids can cause short circuits in equipment such as keyboards.
- Tile floors—Use a dust-absorbent cloth mop rather than a dry mop to clean tile floors.

Figure 2-4 Above Ceiling Ducted Air



Humidity Level

Maintain proper humidity levels. High humidity causes galvanic actions to occur between some dissimilar metals. This eventually causes a high resistance between connections, leading to equipment failures. High humidity can also have an adverse affect on some magnetic tapes and paper media.

Figure 2-3 Ceiling Plenum Air Distribution System

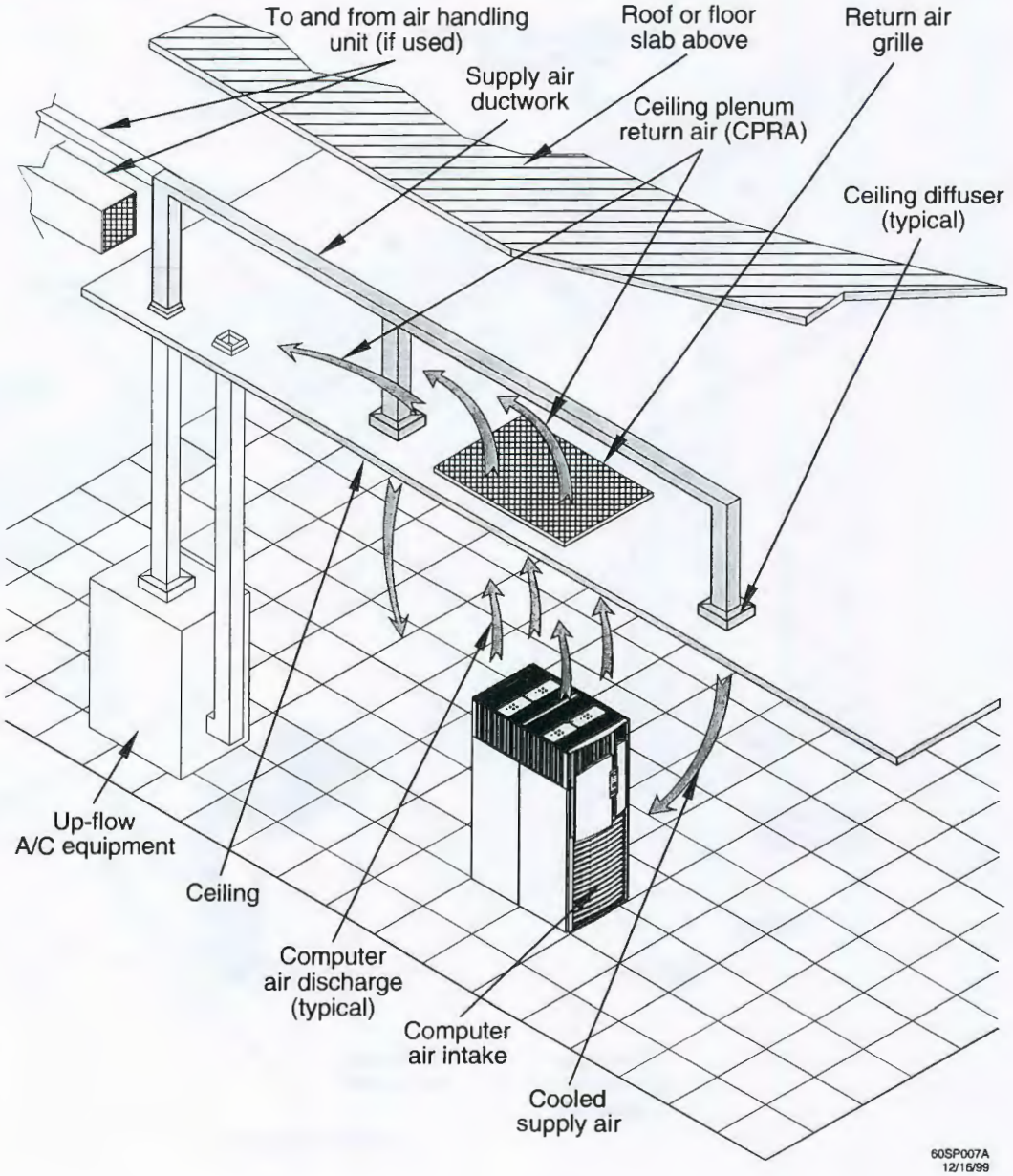
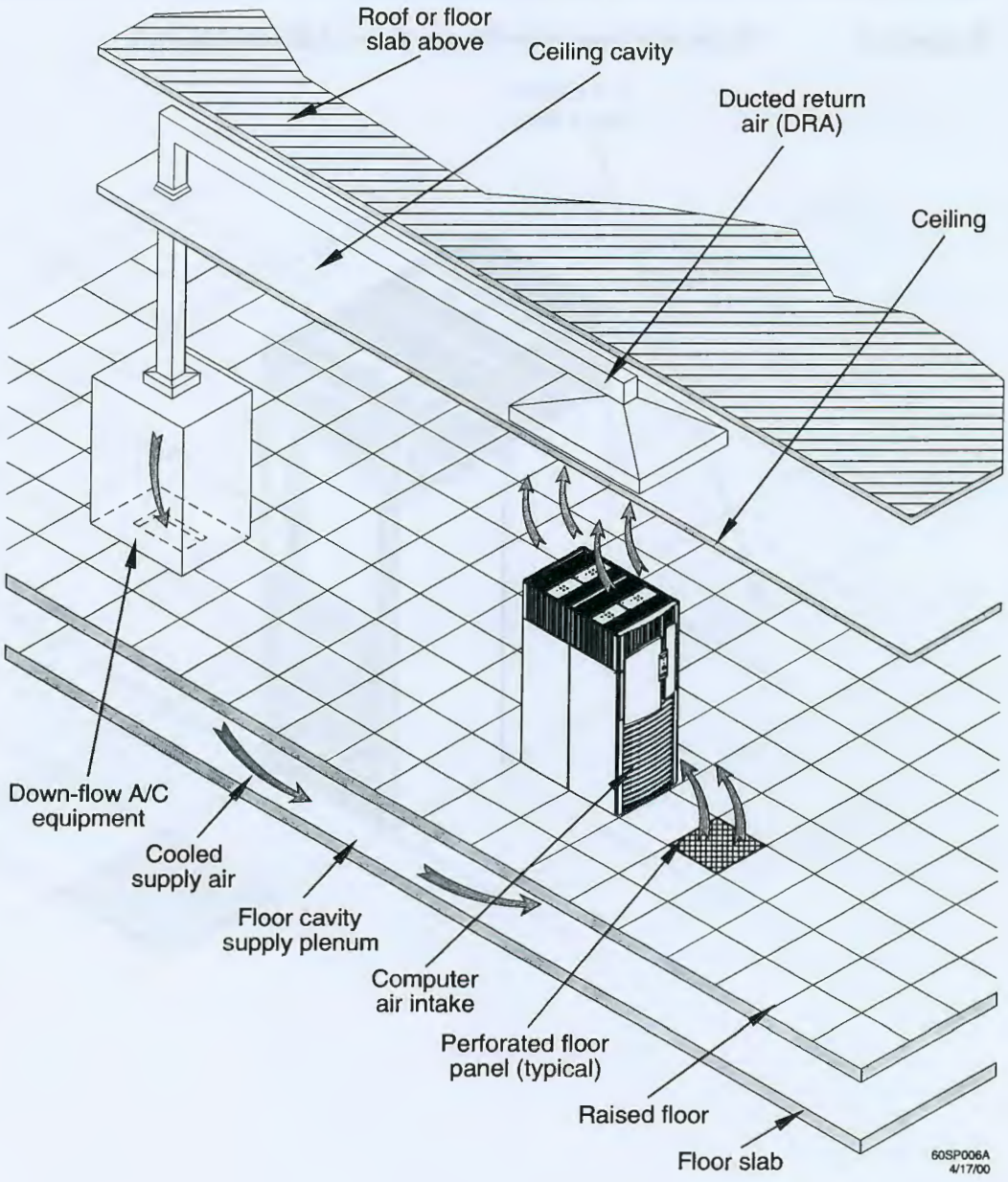


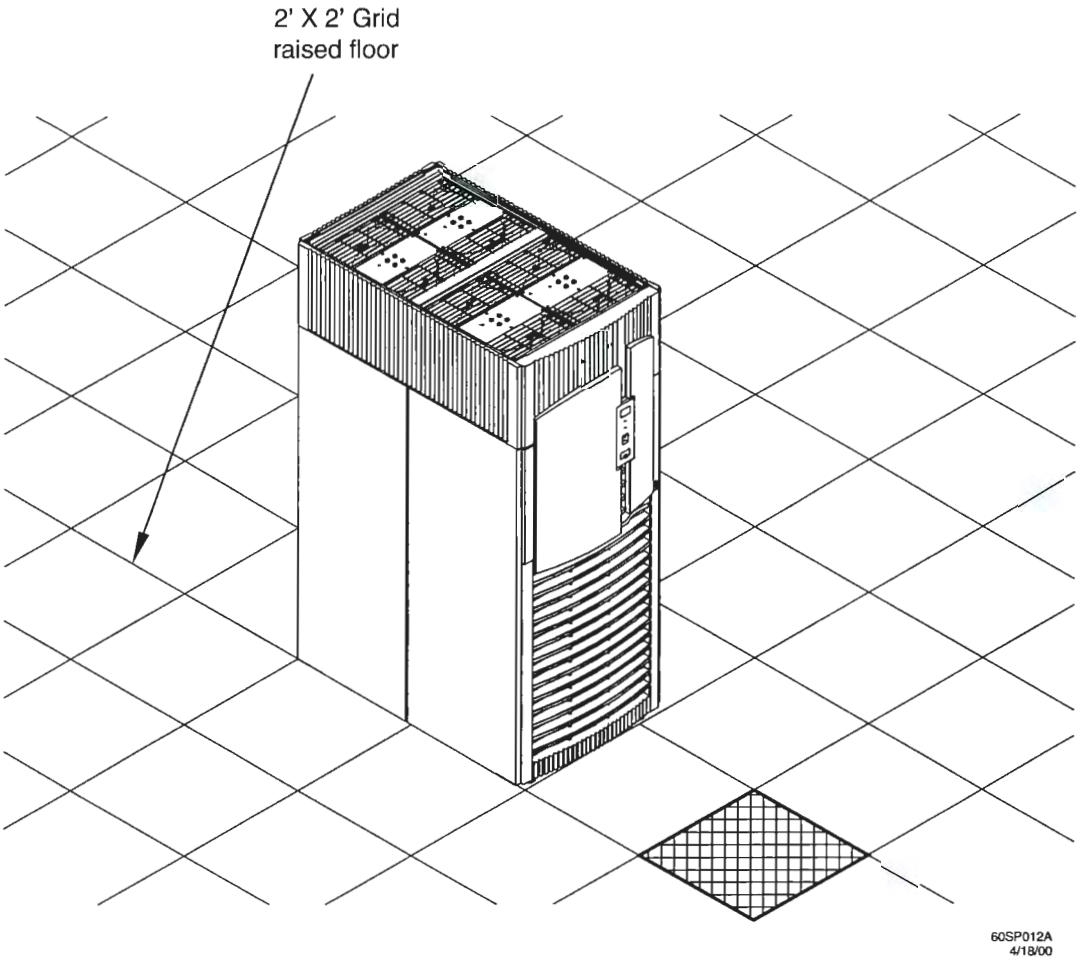
Figure 2-2 Underfloor Air Distribution System



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 756
Doc.

Figure 2-4 on page 50 illustrates a typical computer room above ceiling ducted air distribution system (UFA).

Figure 2-1 Typical Computer Room Raised Floor Layout



Basic Air Distribution Systems

A basic air distribution system includes supply air and return air.

An air distribution system should be zoned to deliver an adequate amount of supply air to the cooling air intake vents of the computer system equipment cabinets. Supply air temperature should be maintained within the following parameters:

- Ceiling supply system—From 55° F (12.8° C) to 60° F (15.6° C)
- Floor supply system—At least 60° F (15.6° C)

If a ceiling plenum return air system or a ducted ceiling return air system is used, the return air grille(s) in the ceiling should be located directly above the computer equipment cabinets.

The following three types of air distribution system are listed in order of recommendation:

- Underfloor air distribution system—Downflow air conditioning equipment located on the raised floor of the computer room uses the cavity beneath the raised floor as plenum for the supply air.

  Return air from an underfloor air distribution system can be ducted return air (DRA) above the ceiling, as shown in Figure 2-2 on page 48.

  Perforated floor panels (available from the raised floor manufacturer) should be located around the perimeter of the system cabinets. Supply air emitted though the perforated floor panels is then available near the cooling air intake vents of the computer system cabinets.

- Ceiling plenum air distribution system—Supply air is ducted into the ceiling plenum from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  The ceiling construction should resist air leakage. Place perforated ceiling panels (with down discharge air flow characteristics) around the perimeter of the system cabinets. The supply air emitted downward from the perforated ceiling panels is then available near the cooling air intake vents of the computer system cabinets.

  Return air should be ducted back to the air conditioning equipment though the return air duct above the ceiling.

- Above ceiling ducted air distribution system—Supply air is ducted into a ceiling diffuser system from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  Return air from an above ceiling ducted air distribution system may be ducted return air (DRA) above the ceiling, as shown in Figure 2-4 on page 50, or ceiling plenum return air (CPRA), as shown in Figure 2-3 on page 49.

  Adjust the supply air diffuser system grilles to direct the cooling air downward around the perimeter of the computer system cabinets. The supply air is then available near the cooling air intake vents of the computer system cabinets.

Air Conditioning System Installation

All air conditioning equipment, materials, and installation must comply with any applicable construction codes. Installation of the various components of the air conditioning system must also conform to the air conditioning equipment manufacturer's recommendations.

Figure 2-2 on page 48 illustrates a typical computer room underfloor air distribution system (DRA).

Figure 2-3 on page 49 illustrates a typical computer room ceiling plenum air distribution system (CPRA).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 757
Doc. 3698

- System controls adequate to maintain the computer room within the operating ranges listed in Table 2-1.

Table 2-1 Computer Room Environment

Parameter	Operating Range	Recommended Range	Maximum Rate of Change (per hour)
Temperature[a,b]	68° to 86° F (20° to 30° C)	68 to 72 °F (20° to 23° C)	9° F repetitive, 36° F nonrepetitive (5° C repetitive, 20° C nonrepetitive)
Humidity	15% - 80% with no condensation (40% - 55% recommended)		6%

a. At altitudes up to 3,000 (9,842) meters.
b. System also requires 2400 CFM airflow.

Lighting and personnel must also be included. For example, a person dissipates about 450 BTUs per hour while performing a typical computer room task.

At altitudes above 10,000 feet (3048 m), the lower air density reduces the cooling capability of air conditioning systems. If your facility is located above this altitude, the recommended temperature ranges may need to be modified. For each 1000 feet (305 m) increase in altitude above 10,000 feet (up to a maximum of 15,000 feet), subtract 1.5° F (0.83° C) from the upper limit of the temperature range listed in Table 1-14 on page 31.

Air Conditioning System Guidelines

The following guidelines are recommended when designing an air conditioning system and selecting the necessary equipment:

- The air conditioning system serveing the computer room should be capable of operating 24 hours a day, 365 days a year. It should also be independent of other systems in the building.
- Consider the long-term value of computer system availability, redundant air conditioning equipment, or capacity.
- The system should be capable of handling any future computer system expansion.
- Air conditioning equipment air filters should have a minimum rating of 45% (based on "AShRA Standard 52-76, Dust Spot Efficiency Test").
- Introduce only enough outside air into the system to meet building code requirements (for human occupancy) and to maintain a positive air pressure in the computer room.

Air Conditioning System Types

The following three air conditioning system types are listed in order of preference:

- Complete self-contained package unit(s) with remote condenser(s). These systems are available with u, or down discharge and are usually located in the computer room.
- Chilled water package unit with remote chilled water plant. These systems are available with up or down discharge and are usually located in the computer room.
- Central station air handling units with remote refrigeration equipment. These systems are usually located outside the computer room.

Environmental Elements

The following environmental elements can affect a Superdome server installation:

- Computer room preparation
- Cooling requirements
- Humidity level
- Air conditioning ducts
- Dust and pollution control
- Electrostatic discharge (ESD) prevention
- Acoustics (noise reduction)
- Zinc whisker control

Computer Room Preparation

The following guidelines are recommended when preparing a computer room for a Superdome server system:

- Locate the computer room away from the exterior walls of the building to avoid the heat gain from windows and exterior wall surfaces.
- When exterior windows are unavoidable, use windows that are double- or triple-glazed and shaded to prevent direct sunlight from entering the computer room.
- Maintain the computer room at a positive pressure relative to surrounding spaces.
- Use a vapor barrier installed around the entire computer room envelope to restrain moisture migration.
- Caulk and vapor seal all pipes and cables that penetrate the envelope.
- Use at least a 12-inch raised floor system for the most favorable room air distribution system (underfloor distribution).
- Ensure a minimum ceiling height of 12 inches between the top of the server and the ceiling. Ensure all ceiling clips are in place.

Cooling Requirements

Air conditioning equipment requirements and recommendations are described in the following sections.

Basic Air Conditioning Equipment Requirements

The cooling capacity of the installed air conditioning equipment for the computer room should be sufficient to offset the computer equipment dissipation loads, as well as any space envelope heat gain. This equipment should include:

- Air filtration
- Cooling or dehumidification
- Humidification
- Reheating
- Air distribution

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Wiring connections must be properly torqued. Many equipment manufacturers specify the proper connection torque values for their hardware.

Ground connections must only be made on a conductive, nonpainted surface. Lockwashers must be used on all connections to prevent connection hardware from working loose.

Data Communications Cables

Power transformers and heavy foot traffic create high energy fields. Route data communications cables away from these areas. Use shielded data communications cables that meet approved industry standards to reduce the effects of external fields. Data cables that are run externally to a metal fire enclosure must have a minimum fire rating of VW-1 or VW-4 or better.

Main Building Electrical Ground The main electrical service entrance equipment should have an earth ground connection, as required by applicable codes. Connections such as a grounding rod, building steel, or a conductive type cold water service pipe provide an earth ground.

Electrical Conduit Ground To provide a continuous grounding system, all electrical conduits should be made of rigid metallic conduit that is securely connected together or bonded to panels and electrical boxes.

Power Panel Ground Each power panel should be grounded to the electrical service entrance with green (green/yellow) wire ground conductors. The green (green/yellow) wire ground conductors should be sized per applicable codes (based on circuit over current device ratings).

NOTE The green wire ground conductor mentioned above may be a black wire marked with green tape.

Computer Safety Ground Ground all computer equipment with the green (green/yellow) wire included in the branch circuitry. The green (green/yellow) wire ground conductors should be connected to the appropriate power panel and should be sized per applicable codes (based on circuit over current device ratings).

Superdome was approved by regulatory agencies around the world, and therefore requires a ground/protective earth. there are no exclusions to this regulatory approval.

High-frequency grounding between IOX and Superdome is provided by the cabinet-to-cabinet signal cabling. Whenever an IOX is connected to a Superdome cabinet, low-frequency grounding between these two cabinets is provided by a ground strap. This ground strap is shipped with each IOX. Refer to the *I/O Expansion Cabinet Guide* for more detail.

Newtwork-connected Equipment Ground The installation must provide a ground connection for the network equipment. This statement is translated into the following two languages as required:

WARNING **Sweden: Apparaten skall anslutas till jordat uttag, när den ansluts till ett nätverk.**

WARNING **Denmark: Før tilslutning af de øvrige ledere, se medfølgende installationsvejledning.**

System Installation Guidelines

This section contains information about installation practices. Some common pitfalls are highlighted. Both power cable and data communications cable installations are discussed.

Wiring Connections

Expansion and contraction rates vary among different metals. Therefore, the integrity of an electrical connection depends on the restraining force applied. Connections that are too tight compress or deform the hardware and causes it to weaken. This usually leads to high impedance causing circuit breakers to trip.

CAUTION Connections that are too loose have a high resistance that cause serious problems, such as erratic equipment operation. A high resistance connection overheats and sometimes causes fire or high temperatures that can destroy hard-to-replace components such as distribution panels or system bus bars.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 759
Doc.

Distribution Hardware

This section describes wire selection and the types of raceways (electrical conduits) used in the distribution system. Wire size is dictated by circuit breaker sizing and local safety codes.

Wire Selection

Use copper conductors instead of aluminum, as aluminum's coefficient of expansion differs significantly from that of other metals used in power hardware. Because of this difference, aluminum conductors can cause connector hardware to work loose, overheat, and fail.

Raceway Systems (Electrical Conduits)

Raceways (electrical conduits) form part of the protective ground path for personnel and equipment. Raceways protect the wiring from accidental damage and also provide a heat sink for the wires.

Any of the following types may be used:

- Electrical metallic tubing (EMT) thin-wall tubing
- Rigid (metal) conduit
- Liquidtight with RFI strain relief (most commonly used with raised floors)
- Plenum-grade cables

Building Distribution

All building feeders and branch circuitry should be in rigid metallic conduit with proper connectors (to provide ground continuity). Conduit that is exposed and subject to damage should be constructed of rigid galvanized steel.

The IOX and Superdome are safety grounded through the green (ground) wire in each AC power cord. In the IOX, this ground passes through the AC power cord entry into the XPC and connects internally to the XPC chassis. The XUC chassis and each ICE chassis are grounded through their respective DC power cords from the XPC. Additional safety grounding must be provided for networking equipment.

Power Routing

Power drops and interface cables from the equipment are routed down from the power panel, through a grommet-protected opening (beneath the floor level), and under the floor panels.

Grounding Systems

Superdome servers require two methods of grounding:

- Power distribution safety grounding
- High frequency intercabinet grounding

Power Distribution Safety Grounding

The power distribution safety grounding system consists of connecting various points in the power distribution system to earth ground using green (green/yellow) wire ground conductors. Having these ground connections tied to metal chassis parts that may be touched protects computer room personnel against shock hazard from current leakage and fault conditions.

Power distribution systems consist of several parts. Hewlett-Packard recommends that these parts be solidly interconnected to provide an equipotential ground to all points.

ECT 8794 Paula CPL-12

The minimum recommended illumination level is 70 foot-candles (756 lumens per square meter) when the light level is measured at 30 inches (76.2 cm) above the floor.

Power Quality

This equipment is designed to operate over a wide range of voltages and frequencies. It has been tested and shown to comply with EMC Specification EN50082. However, damage can occur if these ranges are exceeded. Severe electrical disturbances can exceed the design specifications of the equipment.

Sources of Electrical Disturbances

Electrical disturbances, glitches, affect the quality of electrical power. Common sources of these disturbances are:

- Fluctuations occurring within the facility's distribution system
- Utility service low-voltage conditions (such as sags or brownouts)
- Wide and rapid variations in input voltage levels
- Wide and rapid variations in input power frequency
- Electrical storms
- Large inductive sources (such as motors and welders)
- Faults in the distribution system wiring (such as loose connections)
- Microwave, radar, radio, or cell phone transmissions

Power System Protection

Computer systems can be protected from the sources of many of these electrical disturbances by using:

- A Protective Earth (PE) connection with a wire diameter of at least equal to the current carrying conductors. The neutral conductor must not be used for the PE connection. (The PE wire is GREEN with a YELLOW stripe.)
- A dedicated power distribution system
- Power conditioning equipment
- Over- and under-voltage detection and protection circuits
- Screening to cancel out the effects of undesirable transmissions
- Lightning arresters on power cables to protect equipment against electrical storms

Every precaution has been taken during power distribution system design to provide immunity to power outages of less than one cycle. However, testing cannot conclusively rule out loss of service. Therefore, adherence to the following guidelines provides the best possible performance of power distribution systems for Superdome server equipment:

- Dedicated power source—Isolates server power distribution system from other circuits in the facility.
- Missing-phase and low-voltage detectors—Shuts equipment down automatically when a severe power disruption occurs. For peripheral equipment, these devices are recommended but optional.
- Online uninterruptable power supply (UPS)—Keeps input voltage to devices constant and should be considered if outages of one-half cycle or more are common. Refer to qualified contractors or consultants for each situation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 760
Doc. 3698

Electrical Factors

Proper design and installation of a power distribution system for a Superdome server requires specialized skills. Those responsible for this task must have a thorough knowledge and understanding of appropriate electrical codes and the limitations of the power systems for computer and data processing equipment.

In general, a well-designed power distribution system exceeds the requirements of most electrical codes. A good design, when coupled with proper installation practices, produces the most trouble-free operation.

A detailed discussion of power distribution system design and installation is beyond the scope of this document. However, electrical factors relating to power distribution system design and installation must be considered during the site preparation process.

The electrical factors discussed in this section are:

- Computer room safety
- Electrical load requirements (circuit breaker sizing)
- Power quality
- Distribution hardware
- System installation guidelines

Computer Room Safety

Inside the computer room, fire protection and adequate lighting (for equipment servicing) are important safety considerations. Federal and local safety codes govern computer installations.

Fire Protection

The National Fire Protection Association's Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 75, contains information on safety monitoring equipment for computer rooms.

Most computer room installations are equipped with the following fire protection devices:

- Smoke detectors
- Fire and temperature alarms
- Fire extinguishing system

Additional safety devices are:

- Circuit breakers
- An emergency power cutoff switch
- Devices specific to the geographic location, i.e., earthquake protection

Lighting Requirements for Equipment Servicing

Adequate lighting and utility outlets in a computer room reduce the possibility of accidents during equipment servicing. Safer servicing is also more efficient and, therefore, less costly.

For example, it is difficult to see cable connection points on the hardware if there is not enough light. Adequate lighting reduces the chances of connector damage when cables are installed or removed.

E C T
8196
Paula
CPL - AC

- "Environmental Elements" on page 44 discusses computer room preparation, cooling and humidity requirements, dust and pollution control, electrostatic discharge prevention, and acoustics.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 761
3698
Doc.

2 Electrical and Environmental Guidelines

This chapter provides guidelines for planning and preparing the site. Careful site planning and preparation ensures trouble-free installation and reliable operation of Superdome servers. Factors that may contribute to less than optimal equipment operation are also highlighted.

- "Electrical Factors" on page 39 discusses computer room safety, electrical load requirements, power quality, distribution hardware, and system installation guidelines.

Figure 1-19 Typical Superdome Ceiling Plenum Return Air Cooling System

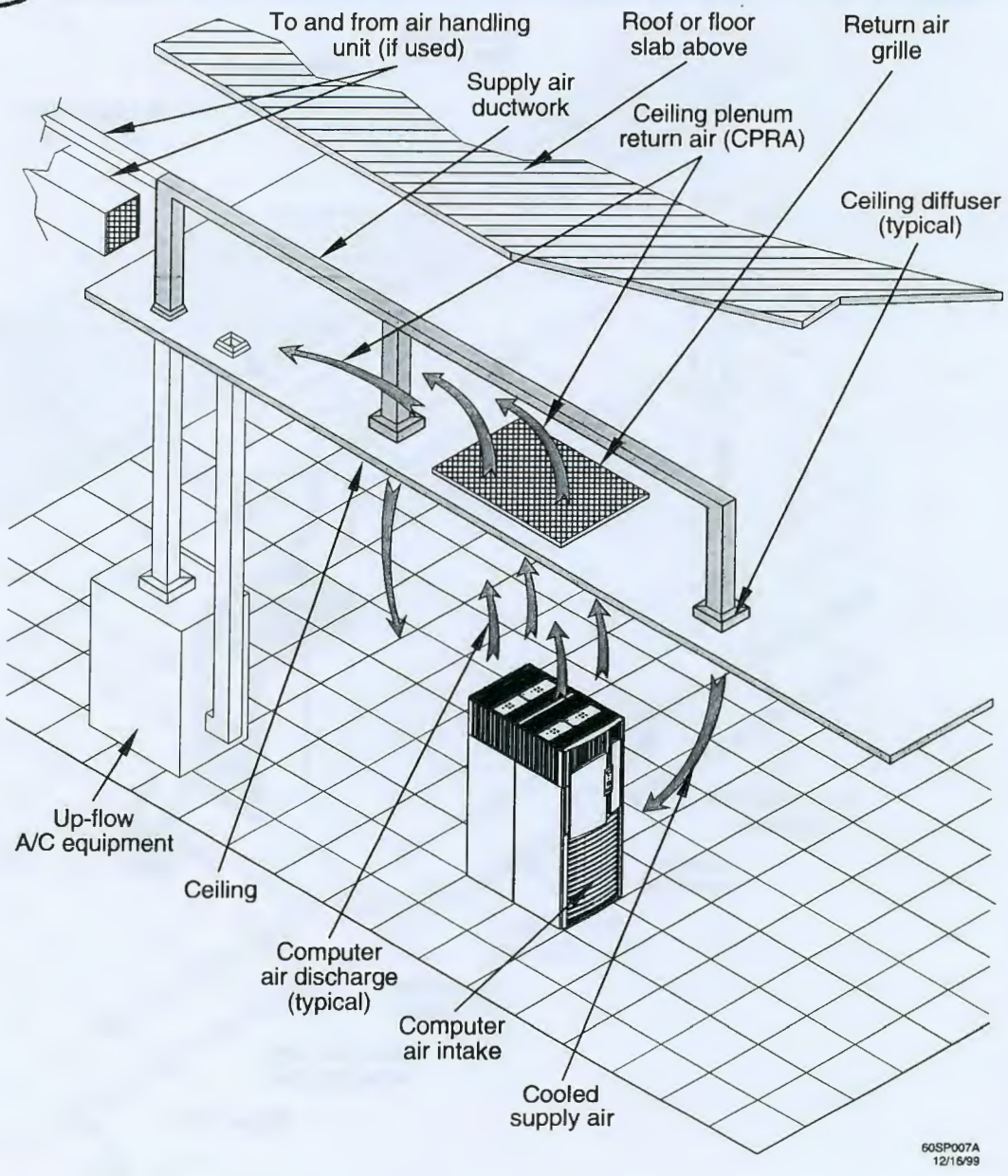


Figure 1-18 Typical Superdome Ducted Return Air Cooling System

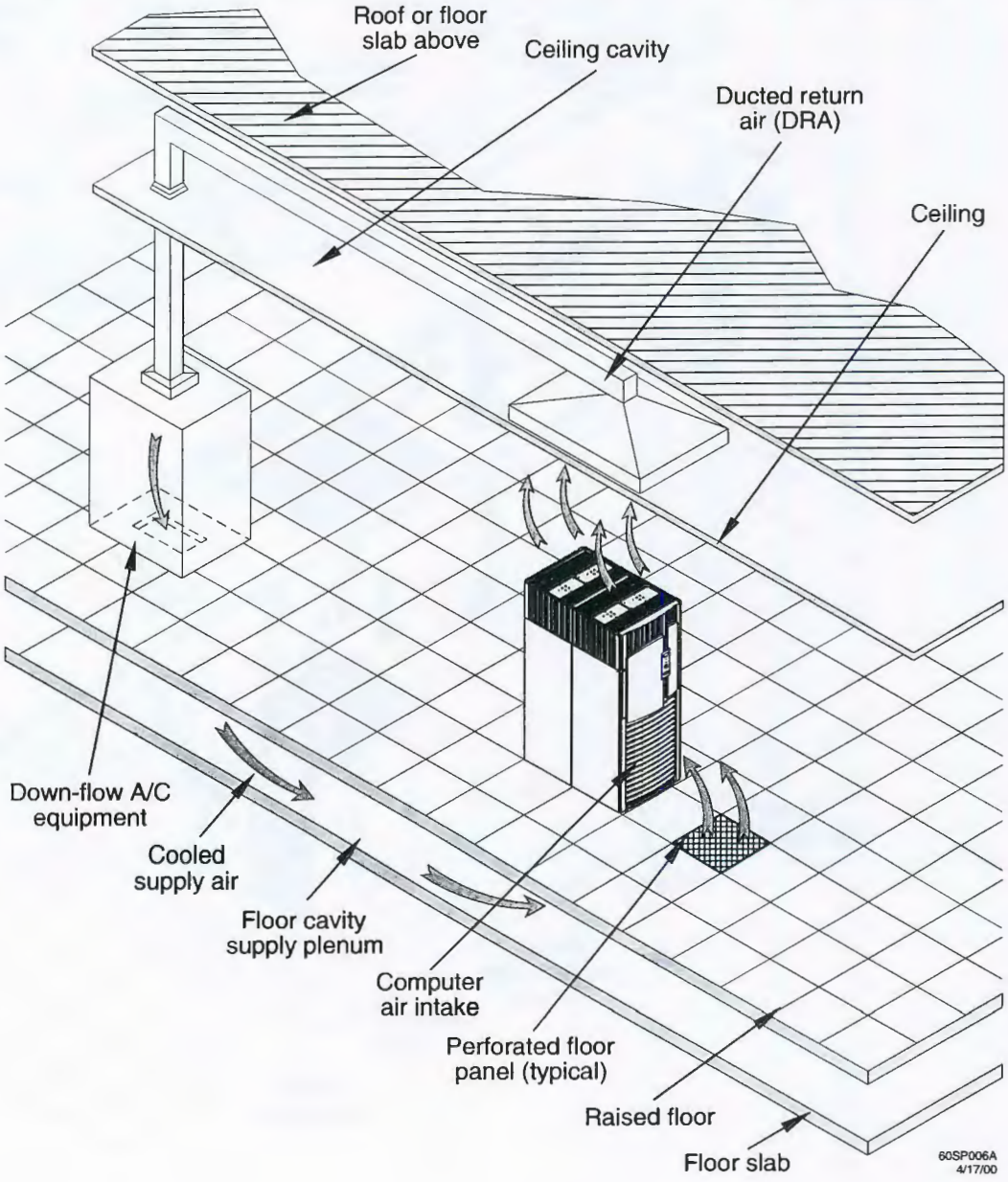
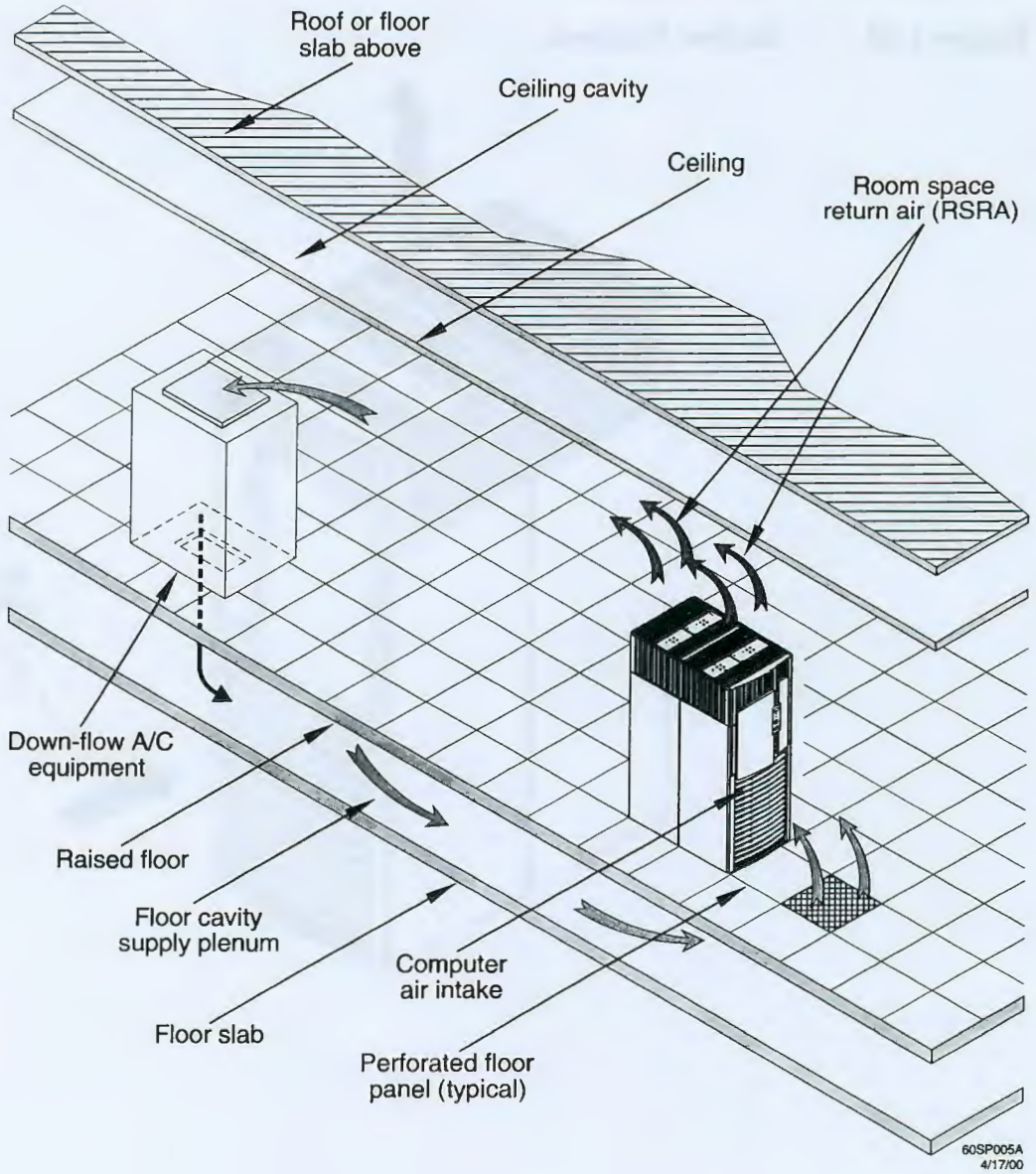


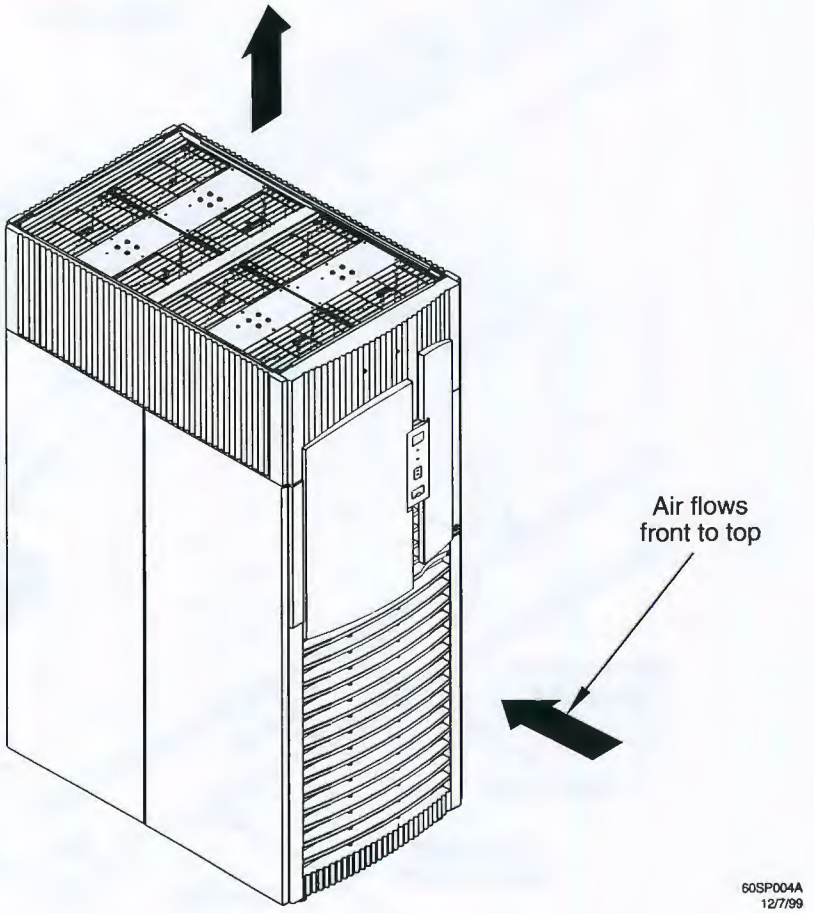
Figure 1-17 Typical Superdome Room Space Return Air Cooling System



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Figure 1-17 on page 34 through Figure 1-19 on page 36 illustrate typical cooling system layouts, adapted from the typical cooling system described in Chapter 2.

Figure 1-16 Airflow Diagram



Support Management Station Power Dissipation

Refer to the applicable documents for the test station power dissipation.

Acoustic Noise Specification

The acoustic noise specification for the Superdome is as follows:

- 8.2 bel (sound power level)
- 65.1 dBA (sound pressure level at operator position)

The above levels are appropriate for dedicated computer room environments, not office environments.

Care should be taken to understand the acoustic noise specifications relative to operator positions within the computer room or when adding Superdomes to computer rooms with existing noise sources.

Air Flow

Superdome requires the cabinet air intake temperature to be between 20o C and 30o C at 2400 CFM. Any cooling system layouts described in Chapter 2 can be adapted to cool the Superdome.

Figure 1-16 on page 33 illustrates the location of the inlet and outlet airducts on a single cabinet.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 764
Doc. 3698

Environmental Requirements

This section provides the environmental, power dissipation, noise emission, and air flow specifications for the Superdome.

Temperature and Humidity Specifications

Ambient intake air temperature is often different from ambient room temperature. You should measure the operating temperature and humidity directly in front of the cabinet cooling air intakes rather than check only ambient room conditions. Table 1-14 lists the computer room temperature and humidity specifications for Superdome servers.

Table 1-14 Computer Room Environment

Parameter	Operating Range	Recommended Range	Maximum Rate of Change (per hour)
Temperature[a],[b]	68° to 86° F (20° to 30° C)	68° to 72 ° F (20° to 25° C)	9° F repetitive, 36° F nonrepetitive (5° C repetitive, 20° C nonrepetitive)
Humidity	15% - 80% with no condensation	40% - 55%	6%

a. At altitudes up to 3,000 (9,842) meters.
b. System also requires 2400 CFM airflow.

At altitudes above 10,000 feet (3048 m), the lower air density reduces the cooling capability of air conditioning systems. If your facility is located above this altitude, the recommended temperature ranges may need to be modified. For each 1000 feet (305 m) increase in altitude above 10,000 feet (up to a maximum of 15,000 feet subtract 1.5° F (0.83° C) from the upper limit of the temperature range listed in Table 1-14.

NOTE Operating ranges refer to the ambient air temperature and humidity measured 0.5 meter from the air intake cooling vents at the same height as these vents.

Power Dissipation

Table E-1 on page 104 shows Superdome power requirements by configuration (i.e. number of cell boards, amount of memory per cell, and number of I/O chassis). This requirement applies to 32-way-capable systems with PA8600 or PA8700 processors.

There are two columns of power numbers (Watts). The Power Breaker column shows the power used to size the wall breaker at the installation site. The Typical Power column shows typical power. Typical power numbers are for PA8600 systems and may be used to assess average utility cost of cooling and electrical power. Expect these typical numbers to be about 18% less for PA8700 systems. Table E-1 on page 104 also shows the recommended breaker sizes for 4-wire and 5-wire sources.

Support Management Station Power Requirements

Refer to the applicable documentation for the SMS power requirements.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

I/O Expansion Cabinet Power Requirements

The I/O expansion cabinet requires a single phase 200-240VAC input. Table 1-11 lists the AC power requirements for the I/O expansion cabinet.

NOTE The IOX accommodates two AC inputs for redundancy

Table 1-11 I/O Expansion Cabinet Power Requirements (without Support Management Station)

Requirements	Value
Nominal input voltage	200-240 VAC
Input voltage range (minimum-maximum)	200-240 VAC
Frequency range (minimum-maximum)	50/60 Hz
Number of phases	1
Marked Electrical input current	16A max
Maximum inrush current	60 A peak
Power factor correction	0.95 minimum

Table 1-12 I/O Expansion Cabinet Component Power Requirements

Power Required (50 - 60 Hz)	VA
Fully configured cabinet	3200
I/O cardcage	500
ICE	600

I/O Expansion Cabinet Power Cords

Table 1-13 lists the power cords for the I/O expansion cabinet.

Table 1-13 I/O Expansion Cabinet AC Power Cords

Part Number A5499AZ	Where Used	Connector Type
-001	North America	L6-20
-002	International	IEC 309

Peripheral Cabinet Power Requirements

There is a high probability that an existing peripheral cabinet may be incorporated into this system. Ensure that adequate power is available for this cabinet and the associated peripherals.

System Power Requirements

Table 1-9 and Table 1-10 list the AC power requirements for a Superdome. These tables provide information to help determine the amount of AC power needed for your computer room.

Table 1-9 Power Requirements (without Support Management Station)

Requirements	Value	Comments
Nominal input voltage	200/208/220/230/240 VAC	
Input voltage range (minimum - maximum)	200 - 240 VAC	Autoselecting (measured at input terminals)
Frequency	50/60 Hz	
Number of phases	3	
Maximum inrush current	90 A peak	
Product Label maximum current, 3-phase, 4-wire	44 A max	Per phase at 200-240VAC
Product Label maximum current, 3-phase, 5-wire	24 A max	Per phase at 200-240VAC
Power factor correction	0.95 minimum	
Ground leakage current (mA)	> 3.5 ma	See WARNING below.

WARNING **Beware of shock hazard. When connecting or removing input power wiring, always connect the ground wire first and disconnect the ground wire last.**

Component Power Requirements

Table 1-9 and Table 1-10 list the AC power requirements for a Superdome. These tables provide information to help determine the amount of AC power needed for your computer room.

Table 1-10 Component Power Requirements (without Support Management Station)

Power Required (50/ 60 Hz)	VA
Maximum configuration Superdome (32-Way)	12,196[a,b]
Cell Board	900
I/O Cardcage	500

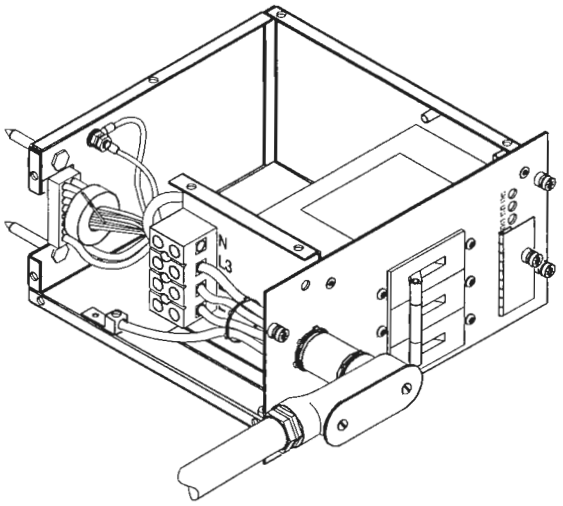
a. A number that should be used for planning to allow for enough power to upgrade through the life of the system.
b. Use Appendix A to determine the actual values required for your system.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 2666
Doc. 3598

Customer Installation Options

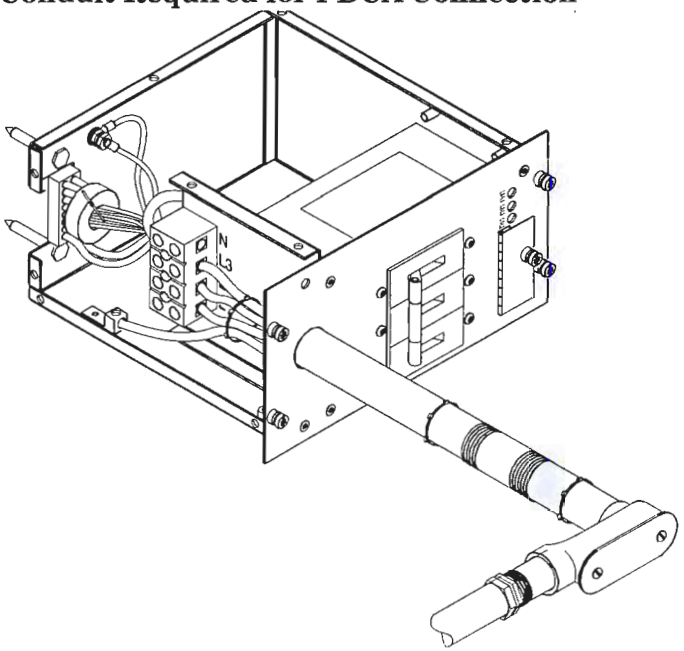
Figure 1-14 and Figure 1-15 detail a suggested configuration for connecting the PDCA when the use of rigid conduit is required or desired. Using a 2- to 4-inch nipple and a 90o elbow allows the conduit to pass through the raised floor at a point immediately past the cabinet. This prevents the conduit from extending beyond the cabinet.

Figure 1-14 PDCA Conduit Connection



60SP046A
8/18/00

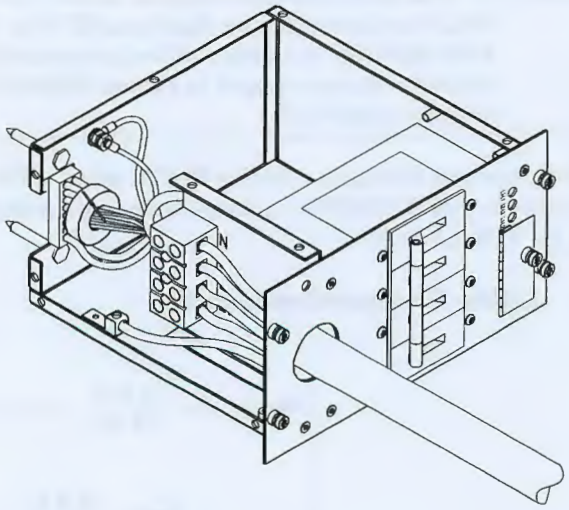
Figure 1-15 Conduit Required for PDCA Connection



60SP045A
8/18/00

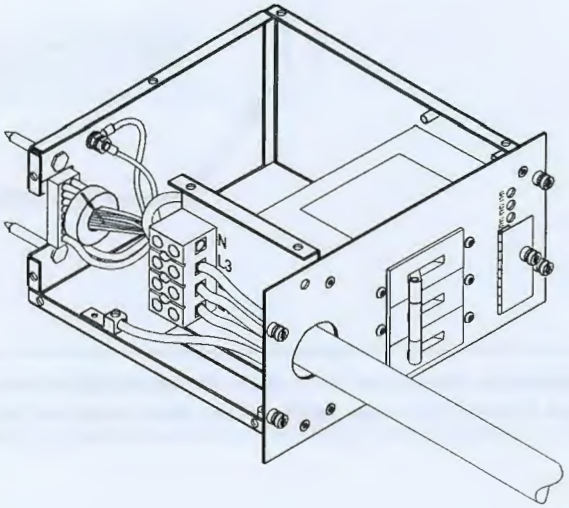
NOTE Figure 1-11 shows a 4-wire cable for illustrative purposes only. 5-wire cable is dimensionally identical regarding insulation and jacket removal. The only exception is the number of conductors.

Figure 1-12 PDCA (Five Wire) Input Wiring Connections



60SP041A
7/13/00

Figure 1-13 PDCA (Four Wire) Input Wiring Connections



60SP041B
9/13/00

RQS nº 09/2005 - CN
CPMI - CORREIOS
Fls Nº 767
Doc.

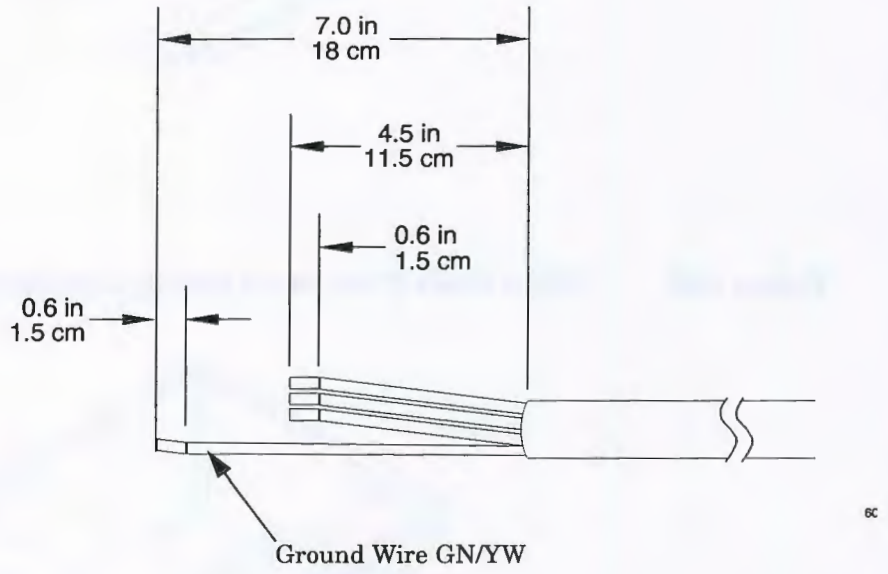
Step 5. Using the five screws retained from the removal procedure, replace the bottom panel on the PDCA. Refer to Figure 1-9 on page 23 for panel installation details.

Step 6. To verify the proper wiring to a 4-wire PDCA, use a DVM to measure the voltage at the test points. Voltage should read 200 - 240 Vac phase-to-phase as measured between the test points as follows: L1 to L2, L2 to L3, L1 to L3.

IMPORTANT In some electrical distributions around the world, it is possible to measure 415 VAC phase-to-phase. Ensure that your DVM is capable of measuring AC voltages of at least 500VAC. A number of 5-wire power distribution systems may have phase-to-phase voltages in excess of 400VAC. Many hand-held volt meters are limited to 300VAC.

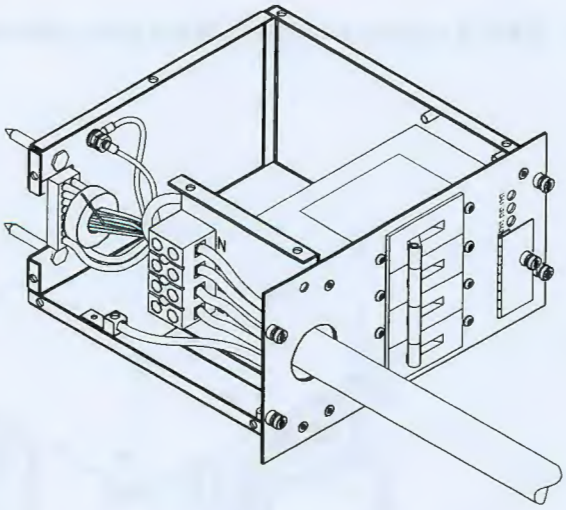
To verify the proper wiring to a 5-wire PDCA, use a DVM to measure the voltage at the test points. Voltage should read 200-240VAC phase-to-neutral, as measured between the test points as follows: L1 to N, L2 to N, L3 to N.

Figure 1-11 Cable Preparation Detail



NOTE Dimensions shown are for a cable strain relief without an extension nipple. If an extension nipple is used, then the cable jacket must removed accordingly.

Figure 1-10 PDCA Input Wiring Connections (5-Wire Unit Shown)



60SP041A
7/13/00

Cable Installation

NOTE These procedures may be used for early deliveries consisting of either option 1 or option 2 as well as those later systems delivered with PDCA cables attached.

Select the proper cable using the following criteria.

- Each Superdome cabinet using a 3-phase, 4-wire input is required to have a four-conductor cable. The four-conductor cable selected by the facility electrician shall be in accordance with local electrical codes to support the selected circuit breaker for the maximum Product Label current of 44A per phase. The facility electrician and local electrical codes will determine proper power cord selection dependent upon desired application such as rigid conduit, flexible conduit, or cable bundle. Observe derating factors for multiple wires per cable.
- Each Superdome cabinet using a 3-phase 5-wire input is required to have a five-conductor cable. The five-conductor cable selected by the facility electrician shall be in accordance with local electrical codes to support the selected circuit breaker for the maximum Product Label current of 24A per phase. The facility electrician and local electrical codes will determine proper power cord selection dependent upon desired application such as rigid conduit, flexible conduit, or cable bundle. Observe derating factors for multiple wires per cable.

Step 1. Prepare the new cable as shown in Figure 1-11 on page 25.

Step 2. Using the cable retaining hardware saved from the cable removal, route the new cable into the PDCA.

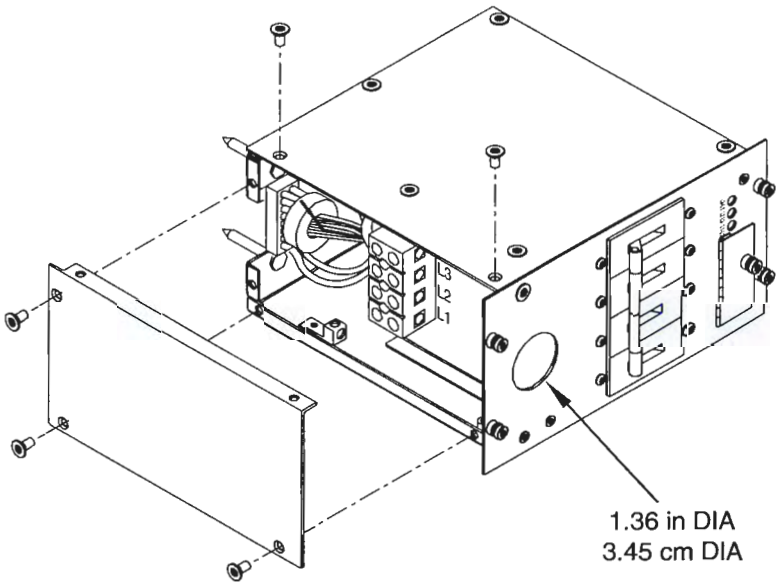
Step 3. Route the cable into the PDCA terminal lugs and secure in position by tightening the lugs.

Step 4. Using the hardware that was retained during the cable removal, attach the green and yellow ground cable.

REQ Nº 03/2005 - CN
CPMI - CORREIOS
765
Fls. Nº
Doc.

Step 5. Remove the cable from the PDCA. Keep all retaining hardware for use during installation of the new cable.

Figure 1-9 PDCA Cable Access (5-Wire Unit Shown)



To remove the existing cable from the PDCA, begin be removing the five T-10 Torx screws detailed in Figure 1-9 on page 23. Then remove the bottom panel of the PDCA. Retain the panel and screws for future use.

NOTE The cable removal and installation requires only the bottom panel to be removed. For image clarity, Figure 1-9 does not show cable or cable strain relief.

Step 1. Locate and remove the PDCAs.

Step 2. Remove the five screws securing the bottom of the PDCA. Retain the screws. Refer to Figure 1-9 for details.

Step 3. Disconnect the existing wires from the PDCA terminal lugs. Refer to Figure 1-9 for details.

NOTE Loosen the cable side terminal lugs only. Do not loosen the PDCA side terminal lugs.

NOTE For 5-wire cables, loosen four lugs. For 4-wire cables, loosen three lugs.

Step 4. Using an 11-mm socket, remove the safety ground cable (green and yellow cable). Retain the attaching hardware.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 769
Doc. 3688

IMPORTANT Ensure that your DVM is capable of measuring AC voltages of at least 500VAC. A number of 5-wire power distribution systems may have phase-to-phase voltages in excess of 400VAC. Many hand-held volt meters are limited to 300VAC.

Figure 1-7 Four-Wire In-Line Connector (A4660A Opt 401)

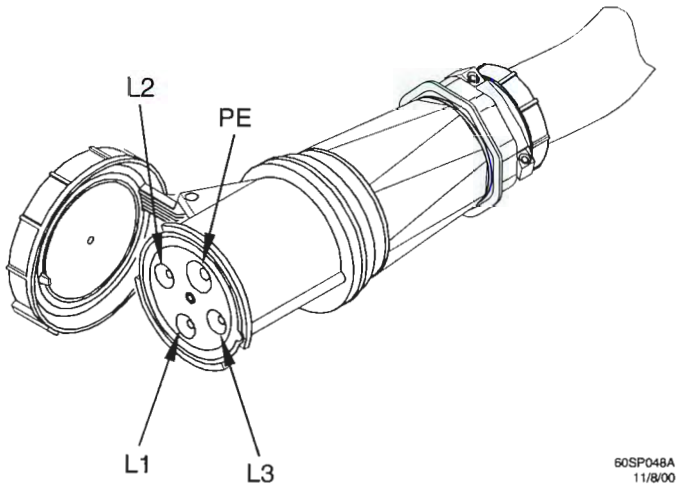
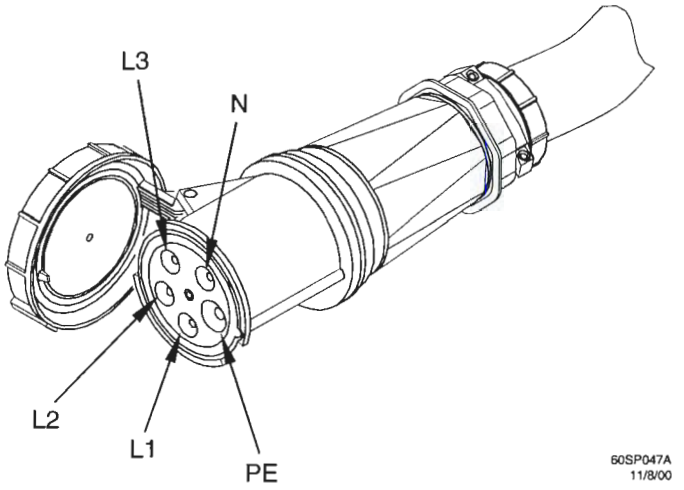


Figure 1-8 Five-Wire In-Line Connector (A4660A Opt 501)



Cable Removal

Some installations may either require or desire that the Superdome(s) be hardwired in lieu of using the standard plugs and connectors provided. In these cases, it is necessary to remove the installed power cable from the PDCA. The following procedures are used to remove and replace the existing power cable.

- To verify the proper wiring for a 4-wire PDCA, use a DVM to measure the voltage at the in-line connector. Voltage should read 200 - 240 Vac phase-to-phase as measured between the connector pins as follows: L1 to L2, L2 to L3, L1 to L3.
- To verify the proper wiring for a 5-wire PDCA, use a DVM to measure the voltage at the connector. Voltage should read 200 - 240 Vac phase-to-neutral as measured between the connector pins as follows: L1 to N, L2 to N, L3 to N.

Figure 1-6 PDCA Assembly for Options 6 and 7 (4-Wire Unit Shown)

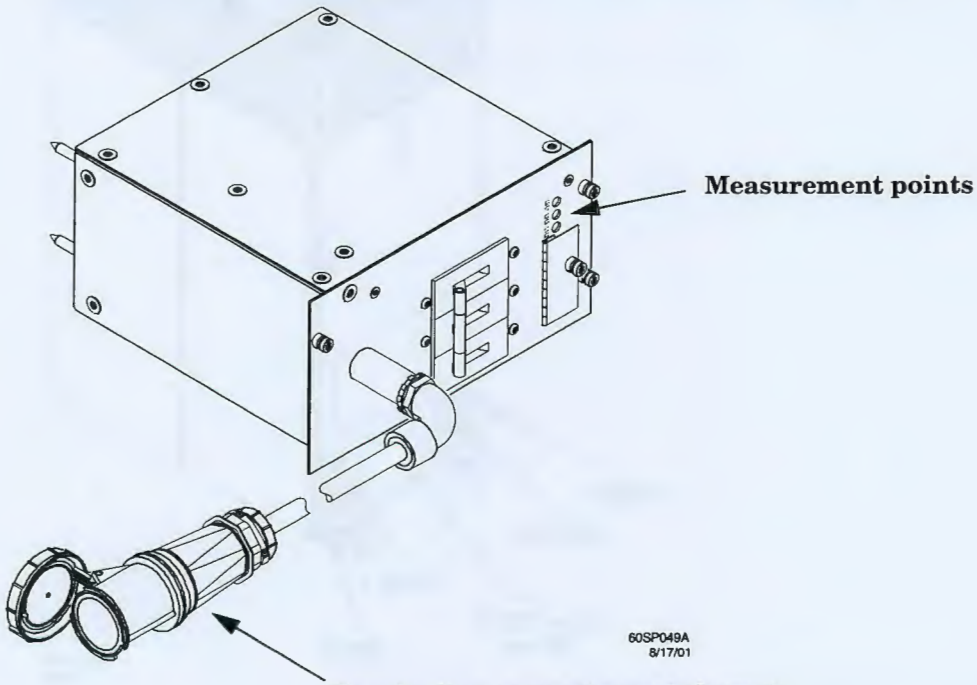
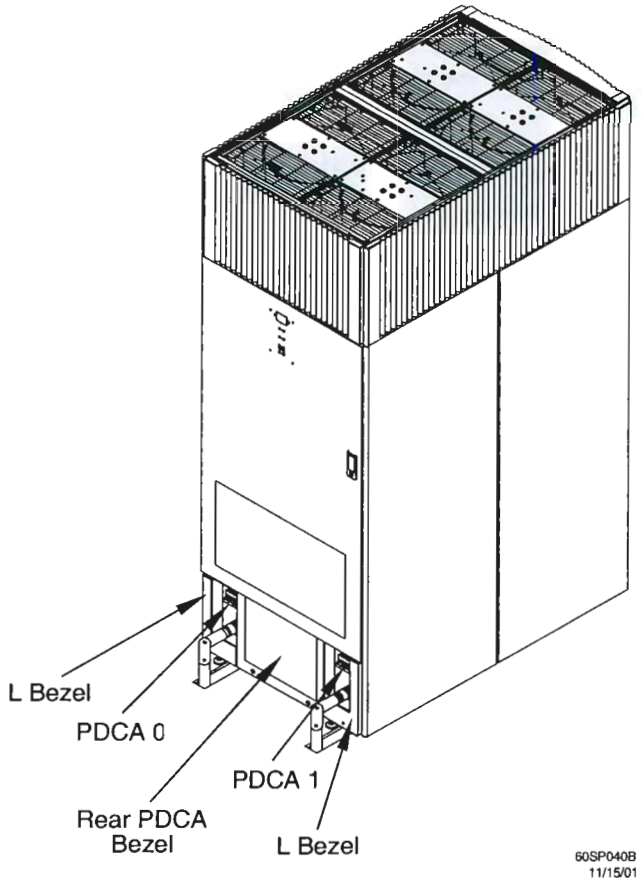


Figure 1-5 PDCA Locations



Power Cords

This section discusses the different possibilities for Superdome PDCA power cords.

Pre-wired PDCAs Options 6 and 7

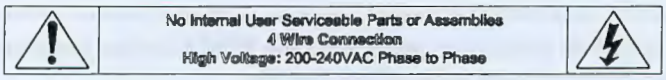
All Superdomes are delivered with the appropriate cable and plug. The mating in-line connector is not provided.

IMPORTANT Verify that the source power is correct for the appropriate PDCA wiring.

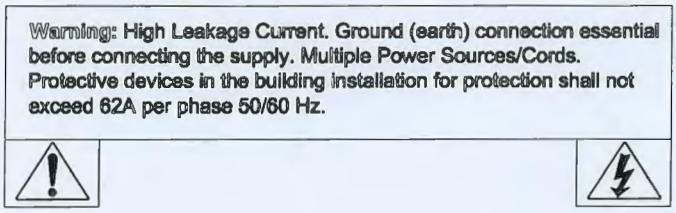
NOTE When installing the power connector, allow enough room for mating the connector with the plug.

Check the voltages at the connector prior to connecting the newly installed connector to the PDCA plug. Refer to Figure 1-7 and Figure 1-8 on page 21 for pin locations.

WARNING **Do not install a PDCA that does not have one of the following set of labels attached.**

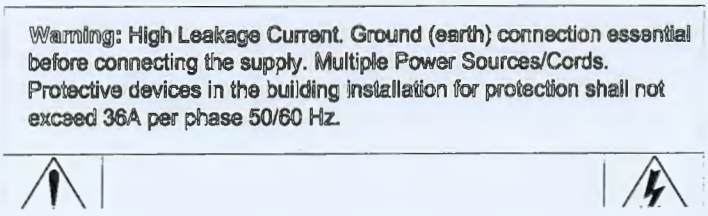


AND



OR

AND



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 611
3698
Doc.

b. Panel-mount receptacles must be purchased by the customer from a local Mennekes supplier.
c. In-line connector is available from HP by purchasing A6440A, Option 501.

NOTE A qualified electrician must wire the PDCA in-line connector to site power using copper wire and in compliance with all local codes.

Each branch circuit used within a Superdome Complex must be connected together to form a common ground.

When only one PDCA is to be installed in a Superdome, it must be installed as PDCA 0. Refer to Figure 1-5 for PDCA 0 location.

j. In the U.S.A., site power is 30 Amps; In Europe site power is 32 Amps.

Table 1-7 Option 004 and 005 Specifics[a]

PDCA Product Number	Attached Power Cord	Attached Plug	Connector Provided
A5800A Option 004	OLFLEX 190 (PN 600404) is a 2.5 meter multi conductor, 600 volt, 90 degree C, UL and CSA approved, oil resistant flexible cable. (100 A capacity)	Mennekes ME 4100P9 (100 A capacity)	Mennekes ME 4100C9 (100 A capacity)
A5800A Option 005	H07RN-F (OLFLEX PN 1600111) is a 2.5 meter heavy duty neoprene jacketed harmonized European flexible cable. (63 A capacity)	Mennekes ME 563P6-1235 (63 A capacity)	Mennekes ME 563C6-1245 (63 A capacity)

a. Options 4 and 5 have been deleted.

Table 1-8 Options 006 and 007 Specifics

			Customer-Provided Part	
PDCA Product Number	**Attached Power Cord**	**Attached Plug**	**In-Line Connector**	**Panel-Mount Receptacle**
A5800A Option 006	OLFLEX 190 (PN 600804), four-conductor, 6-AWG (16-mm^2), 600-Volt, 60-Amp, 90-degree C, UL, and CSA approved, conforms to CE directives GN/YW ground wire.	Mennekes ME 460P9 3-phase, 4-wire, 60-amp, 250-volt, UL approved. color blue, IEC 309-1, IEC 309-1, grounded at 3:00 o'clock.	Mennekes ME 460C9 3-phase, 4-wire, 60-amp, 250-volt, UL approved. color blue, IEC 309-1, IEC 309-1, grounded at 9:00 o'clock.[a]	Mennekes ME 460R9 3-phase, 4-wire, 60-amp, 250-volt, UL approved. color blue, IEC 309-1, IEC 309-1, grounded at 9:00 o'clock.[b]
A5800A Option 007	Five conductors, 10-AWG (6-mm^2), 450/475-volt, 32-amp, <HAR> European wire cordage, GN/YW ground wire.	Mennekes ME 532P6-14 3-phase, 5-wire, 32-amp, 450/475-volt, VDE certified, color red, IEC 309-1, IEC 309-2, ground at 6:00 o'clock.	Mennekes ME 532C6-16 3-phase, 5-wire, 32-amp, 450/475-volt, VDE certified, color red, IEC 309-1, IEC 309-2, ground at 6:00 o'clock.[c]	Mennekes ME532R6-1276 3-phase, 5-wire, 32-amp, 450/475-volt, VDE certified, color red, IEC 309-1, IEC 309-2, ground at 6:00 o'clock.[b]

a. In-line connector is available from HP by purchasing A6440A, Option 401.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Table 1-6 Available Power Options (Continued)

PDCA Product Number	Source Type	Source Voltage (nominal)	PDCA Required	Input Current Per Phase 200-240 VAC	In-line Connector Required
A5800A Option 005[d]	3-phase	Voltage range 200-240 VAC, phase-to-neutral, 50/60 Hz (EUR typical)	5-wire	24A Maximum per phase	In-line connector and plug provided with a 2.5-meter power cable. Electrician must hard-wire in-line connector to 60/63A site power.[c,e,f]
A5800A Option 006[g]	3-phase	Voltage range 200-240 VAC, phase-to-phase, 50/60 Hz	4-wire	44A Maximum per phase	2.5meter UL power cord and UL approved plug provided. The customer must provide the mating in-line connector or purchase quantity one A6440A opt 401 to receive a mating inline connector. An electrician must hard wire the in-line connector to 60A/63A site power.[c,f,h]
A5800A Option 007[i]	3-phase	Voltage range 200-240 VAC. phase-to-neutral. 50/60 Hz	5-wire	24A Maximum per phase	2.5meter <HAR> power cord and VDE approved plug provided. The customer must provide the mating in-line connector or purchase Quantity 1 A6440A opt 501 to receive a mating in line connector. An electrician must hard wire the in-line connector to 30A/32A site power.[c,h,i]

a. Options 1 and 2 have been deleted.
b. 415 VAC phase-to-phase is possible.
c. A dedicated branch is required for each PDCA installed.
d. Options 4 and 5 have been deleted.
e. Refer to Table 1-7 for detailed specifics related to this option.
f. In the U.S.A., site power is 60 Amps; In Europe site power is 63 Amps.
g. Customer must provide in-line connector or purchase A6440A option 401.
h. Refer to Table 1-8 for detailed specifics related to this option.
i. Customer must provide in-line connector or purchase A6440A option 501.

Example 1-1 **The customer has a 3-phase source with a Source Voltage of 208 VAC measured phase-to-phase indicating that a 4-wire PDCA is required.**

Example 1-2 **The customer has a 3-phase source with a Source Voltage of 220 VAC measured phase-to-neutral indicating that a 5-wire PDCA is required.**

Example 1-3 **The customer has a 3-phase source with a Source Voltage of 230 VAC measured phase-to-phase indicating that a 4-wire PDCA is required.**

Example 1-4 **The customer has a 3-phase source with a source voltage of 415 VAC measure phase-to-phase and a measured phase-to-neutral source voltage of 240 VAC, indicating a 5-wire PDCA is required.**

Input Power Options

Table 1-6 describes the available power options:

Table 1-6 Available Power Options

PDCA Product Number	Source Type	Source Voltage (nominal)	PDCA Required	Input Current Per Phase 200-240 VAC	In-line Connector Required
A5800A Option 001[a]	3-phase	Voltage range 200-240 VAC, phase-to-neutral, 50/60 Hz (EUR typical)[b]	5-wire	24A Maximum per phase	None required. Electrician must hard wire power to the PDCA[c]
A5800A Option 002[a]	3-phase	Voltage range 200-240 VAC, phase-to-phase, 50/60 Hz (US typical)	4-wire	44A Maximum per phase	None required. Electrician must hard-wire power to the PDCA[c]
A5800A Option 004[d]	3-phase	Voltage range 200-240 VAC, phase-to-phase, 50/60 Hz (US typical)	4-wire	44A Maximum per phase	In-line connector and plug provided with a 2.5-meter power cable. Electrician must hard-wire in-line connector to 100A site power.[c,e]

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1773
Doc.

Electrical Specifications

This section provides electrical specifications for Superdomes.

Grounding

The site building shall provide a safety ground/protective earth for each AC service entrance to all Superdome cabinets.

This equipment is CLASS 1 and requires full implementation of the grounding scheme to all equipment connections. Failure to attach Protective Earth results in loss of regulatory compliance and creates a possible safety hazard.

Circuit Breaker

Each Superdome cabinet using a 3-phase, 4-wire input requires dedicated circuit breaker to support the Marked Electrical current of 44A per phase. The facility electrician and local service codes will determine proper circuit breaker selection.

Each Superdome cabinet using a 3-phase 5-wire input requires a dedicated circuit breaker to support the Marked Electrical current of 24A per phase. The facility electrician and local service codes will determine proper circuit breaker selection.

NOTE See Table E-1 on page 104 for systems that are configured with less than a full compliment of cell boards, memory, and I/O modules.

NOTE When using the minimum sized breaker, always choose circuit breakers with the maximum allowed trip delay to avoid nuisance tripping.

NOTE As of March, 2002, PDCA Options 4 and 5 are obsolete.

Detailed site power information is required to configure the system correctly and prevent delays in system installation. Collect the following information from the customer site electrician before selecting the appropriate PDCA.

- Type of source available 4-wire_____ 5-wire_____
- Source voltage phase-to-phase _____ Vac
- Source voltage phase-to-neutral _____Vac

Using the above information, determine the appropriate power option from Table 1-6.

1. Select the source type that matches the customer source.
2. Within the matching Source Type selection, select the matching voltage range to the customer's source voltage.
3. Select the appropriate PDCA.
4. The customer must either provide the correct mating in-line connector or order one from HP. See Table 1-8 for details.

Shipping Dimensions and Weights

Table 1-5 lists the dimensions and weights of the Support Management Station and the Superdome cabinet with shipping pallet.

Table 1-5 Miscellaneous Dimensions and Weights

Equipment	Width (cm)	Depth/Length (cm)	Height (cm)	Weight (kg)
Superdome on shipping pallet[a b c]	39.00 in (99.06)	48.63 in (123.5)	73.25 in (186.7)	1360.8lbs (618.54)
Blowers/Frame on shipping pallet	40.00 in (101.6)	48.00 in (121.9)	62.00 (157.5)	99.2 lbs (45.01)
I/O Expansion cabinet on shipping pallet [d]	38.00in (96.52)	48.00 in (121.9)	88.25 in (224.1)	1115 lbs (505.8)

a. Shipping box, pallet, ramp, and container adds approximately 116 lbs (52.63 kg) to the total system weight.
b. Blowers/Frame are shipped on a separate pallet.
c. Size and number of miscellaneous pallets are determined by the equipment ordered by the customer.
d. Assumes no I/O cards or cables installed. The shipping kit and pallet and all I/O cards adds approximately 209 lbs to the total weight.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº Chapter 1
Doc.

Component Weights

Table 1-3 lists the server and component weights. To determine the overall weight of your specific system, see Table A-1 on page 80 and Table A-2 on page 81.

NOTE Refer to the appropriate documents to determine the weight of the SMS and any console that will be used with this server.

Table 1-3 System Component Weights

Component	Quantity	Weight (kg)
Chassis[a]	1	745.17 lbs (338.10)
Cell Board	8	328.00 lbs (148.82)
DIMMs	256	51.20 (23.27)
Bulk Power Supply (BPS)	6	23.00 lbs (10.44)
PDCA	2	52.00 lbs (23.59)
I/O cardcage	4	146.00 lbs (66.24)
I/O Cards	48	21.60 (9.80)
Fully configured server (32-way cabinet)	1	1366.97 lbs (621.35)[b]

a. The listed weight for a chassis includes the weight of all components not listed in Table 1-3.
b. The listed weight for a fully configured cabinet includes all components and quantities listed in Table 1-3.

Table 1-4 I/O Expansion Cabinet Weights

Component	Weight[a] (kg)
Fully configured cabinet	1104.9 lbs (502.2)
I/O cardcage	36.50 lbs (16.56)
Chassis	264 lbs (120)

a. The listed weight for a fully configured cabinet includes all items installed in a 1.6 meter cabinet. Add approximately 11 lbs when using a 1.9 meter cabinet.

Dimensions and Weights

This section provides dimensions and weights of the system components.

Component Dimensions

Table 1-1 lists the dimensions for the cabinet and components of a Superdome.

Table 1-1 Server Component Dimensions

Component	Width (cm)	Depth/ Length (cm)	Height (cm)	Maximum Quantity per Cabinet
Cabinet	30 (76.2)	48 (121.9)	77.2 (195.6)	1
Cell board (HCB)	16.5 (41.9)	20.0 (50.2)	3.0 (7.6)	8[a]
Cell board power board (HCPB)	16.5 (41.9)	10.125 (25.7)	3.0 (7.6)	8a
I/O backplane (HIOB)	11 (27.9)	17.6 (44.7)		1
Master I/O backplane (HMIOB)	3.25 (8.3)	23.75 (60.3)	1.5 (3.8)	1
I/O cardcage	12.0 (30.5)	17.5 (44.4)	8.38 (21.3)	4
PDCA	7.5 (19.0)	11.0 (27.9)	9.75 (24.3)	2

a. Superdome 16 Way is limited to a maximum of 4.

Table 1-2 I/O Expansion Cabinet Component Dimensions

Component	Width (cm)	Depth/ Length (cm)	Height (cm)	Maximum Quantity per Cabinet
Cabinet	24.0 (61.0)	53.2 (135.1)	77.3 (196.0)	1
ICE	17.6 (44.8)	33.5 (82.0)	16.2 (39.7)	3
I/O cardcage	12.0 (30.5)	17.5 (44.4)	8.38 (21.3)	6

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Upgrading Superdomes and Server Systems

This section provides the details relating to upgrading a Superdome.

IMPORTANT Ensure that the customer is aware of the iCOD email requirements. That is, each bootable partition requires a connection to the internet to send email to notify Hewlett-Packard that the customer has allocated additional CPUs beyond the amount initially purchased. Each bootable partition must be configured to perform this operation.

For more details, go to http://superdome.hp.com and click on the iCOD link.

Upgrading the Server

Space requirements remain the same, but power and cooling must be increased when upgrading within a cabinet (adding additional cells, I/O, etc.).

Special attention should be given to the original circuit breaker and wiring sizes to ensure safety compliance and margins are sill appropriate.

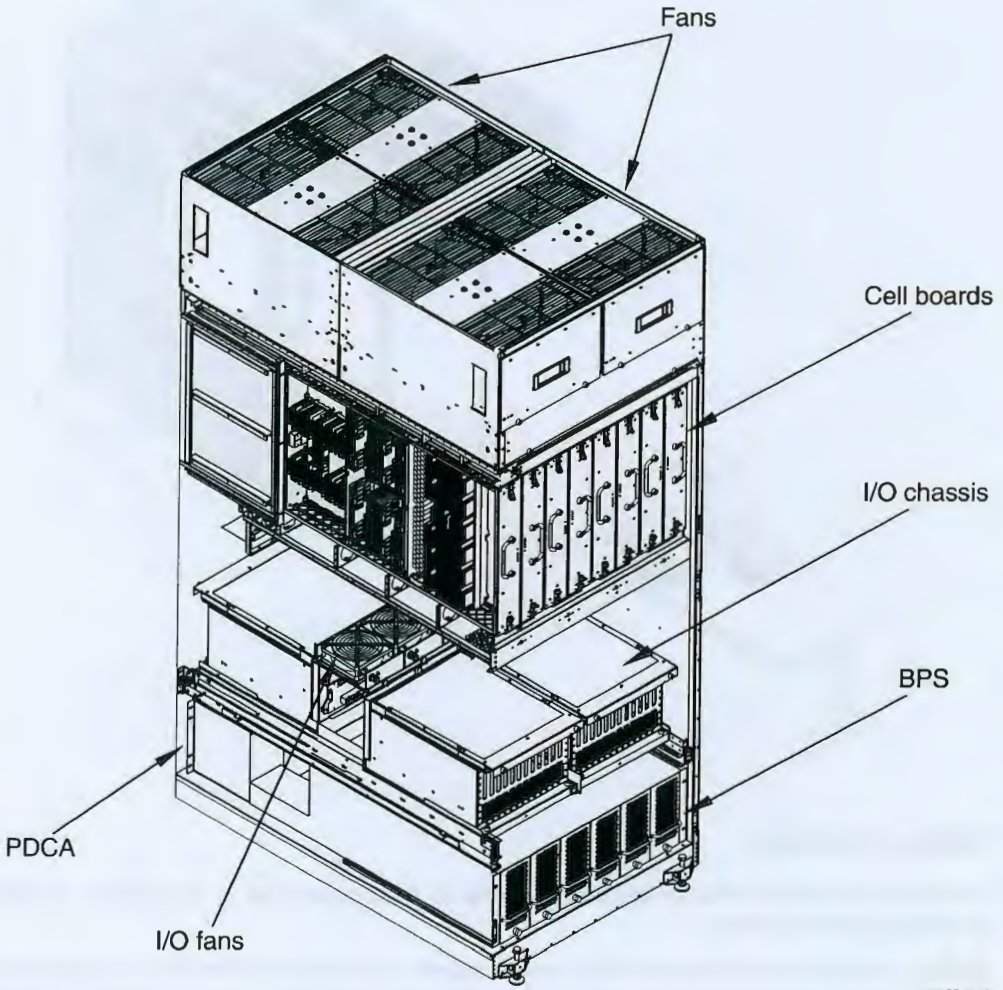
Identify and plan for future upgrades and expansions. It is cost effective to provide the cooling and power capability now for potential future expansions.

Upgrading the System

Space, power, and cooling requirements must be considered and increased as necessary when upgrading a Superdome (adding additional cabinets, cells, I/O, etc.).

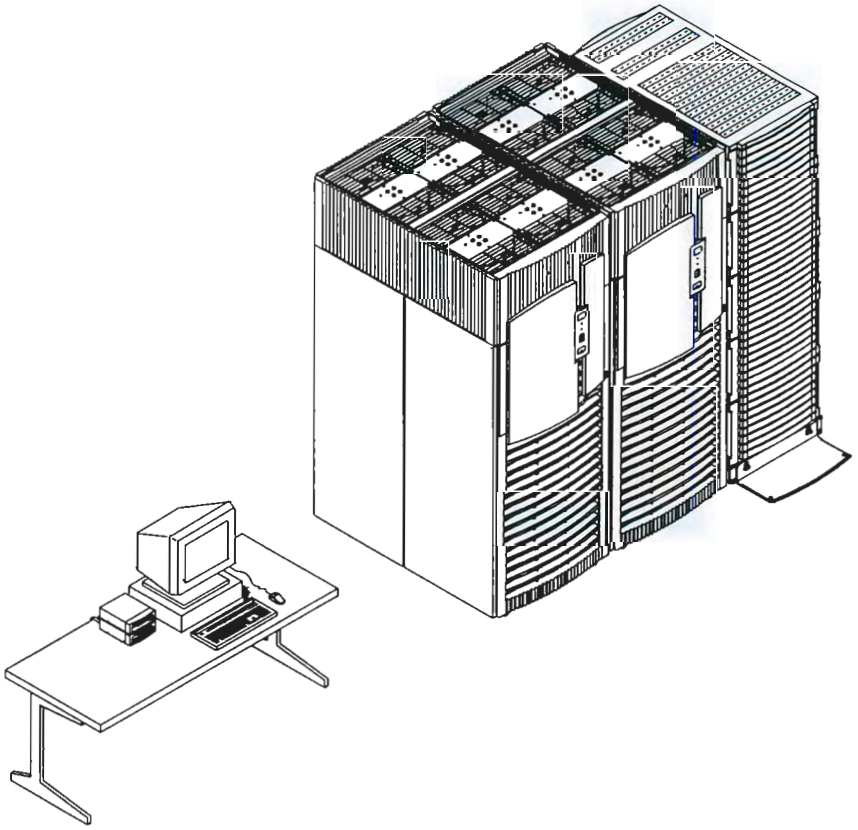
A single cabinet Superdome 16 Way may contain up to four cell boards (16 processors), four I/O card cages, six I/O fans, four system cooling fans, four bulk power supplies, and two PDCA. Additionally, to the above, two backplane power supplies provides N+1 for the Superdome 16 Way.

Figure 1-4 Server Cabinet Components



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 776
Doc.

Figure 1-3 Typical Superdome 64 Way Superdome and I/O Expansion Cabinet Installation



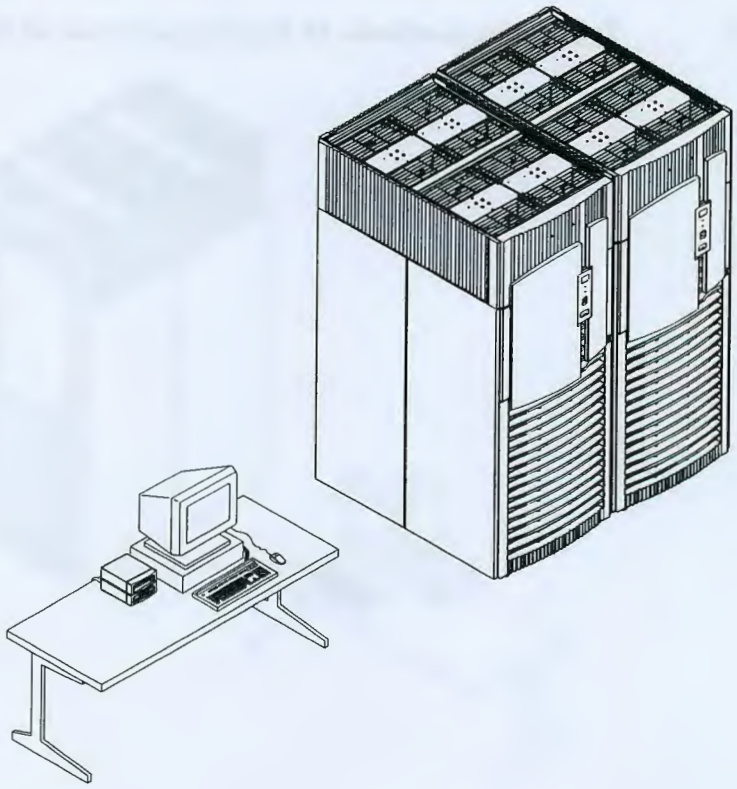
60SP003A
4/26/00

Server Cabinet

The server cabinet is the main building block of the Superdome. A Superdome 64 Way comprises two server cabinets interconnected.

A single cabinet Superdome 32 Way may contain up to eight cell boards (32 processors), four I/O card cages, six I/O fans, four system cooling fans, six bulk power supplies, and two PDCA. Figure 1-4 illustrates the location of these components.

Figure 1-2 Typical Superdome 64 Way Superdome Installation

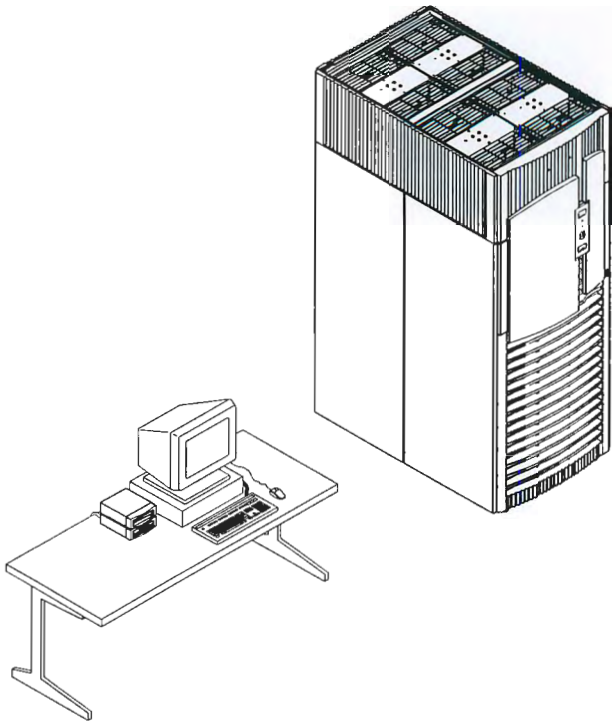


60SP002A
4/17/00

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Figure 1-3 on page 7 illustrates a typical Superdome 64 Way and I/O expansion cabinet installation.

Figure 1-1 Typical Superdome 16 Way/Superdome 32 Way Installation



60SP001A
4/17/00

Server System

This section provides an overview of the basic system building blocks of a Superdome.

Basic System Building Blocks

The basic system building blocks used to configure a Superdome are as follows:

- Server cabinet
- Support Management Station

Figure 1-1 on page 5 illustrates a typical Superdome 16 Way/Superdome 32 Way installation.

Figure 1-2 on page 6 illustrates a typical Superdome 64 Way installation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 770
Doc.

General

This chapter lists the specifications of a Superdome. Throughout this chapter each specification is defined as thoroughly as possible to ensure that all data is considered to ensure a successful site preparation.

"Server System" on page 4 describes the basic system building blocks.

- "Upgrading Superdomes and Server Systems" on page 9 discusses the additional requirements resulting from upgrading Superdomes.
- "Dimensions and Weights" on page 10 discusses the physical size and weight of the Superdome components.
- "Electrical Specifications" on page 13 discusses the power requirements for the system and Support Management Station.
- "Environmental Requirements" on page 31 discusses temperature and humidity, power dissipation, and air flow information about the server and Support Management Station.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 779
Doc.

1 System Specifications

The following Superdome specifications are based on HP Environmental Class C2. Class C2 is a controlled computer room environment where products are subject only to controlled temperature and humidity extremes.

This chapter describes the basic Superdome configuration including physical specifications and requirements:

ECT
8835
Paula
CPL - AC

xx

RQS nº 03/2005 - CN
CPMI -- CORREIOS
Fls. Nº 780
Doc.

Figure 12 I/O Expansion Cabinet Declaration of Conformity Page 2

FCC Regulations (USA Only)

The Federal Communications Commission (in 47 CFR Part 15) has specified that the following notice be brought to the attention of the users of this product.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance (Hewlett-Packard) could result in the equipment being non-compliant with the FCC Class A requirements and void the user's authority to operate the equipment.

Additional International Approvals

AS/NZS 3548:1995 C-Tick & Supplier Code (N279)	Australia/New Zealand
CSA C22.2 No. 60950:2000	Canada
ICES-003 Issue 3	Canada
VCCI Class A	Japan
BSMI, CNS-13438 11/94(Rev. 5/97)	Taiwan
MIC No. 1996-18, Class A	Korean
GB4943-1995	China
GB9254-1988	China

IEC 60950 Evaluated for Country National Differences

CENELEC, AT = Austria, AU = Australia, BE = Belgium, CA = Canada, CH = Switzerland, CN = China, CZ = Czech Republic, DE = Germany, DK = Denmark, ES = Spain, FI = Finland, FR = France, GB = United Kingdom, GR = Greece, HU = Hungary, IE = Ireland, IL = Israel, IN = India, IT = Italy, JP = Japan, KR = Republic of Korea, NL = The Netherlands, NO = Norway, PL = Poland, RU = Russia, SE = Sweden, SG = Singapore, SI = Slovenia, SK = Slovakia, TR = Turkey, UA = Ukraine, US = United States, ZA = South Africa

Figure 11 I/O Expansion Cabinet Declaration of Conformity Page 1

DECLARATION OF CONFORMITY

according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name:	Hewlett-Packard Company
Address:	3000 Waterview Parkway Richardson, TX 75080, USA

Declares that the product:

Product Name:	I/O Expansion (IOX) cabinet for SuperDome
Model Number(s):	SPP6:IOX, SPP6-1:XPC, SPP6-2:XUC/RDM, SPP6-3:ICE
Base Product Number(s):	A5861A:IOX, A5861-26001:XPC, A5861-26002:XUC, A5861-26003:RDM, A5862A:ICE
Product Option(s):	All

Conforms to the following Product Specifications:

Safety: IEC 60950:1999 (with national differences for the countries listed on page 2)
EN 60950:2000
UL 60950:2000

EMC:	CISPR 22 3rd edition:1997/ EN 55022:1998	Class A
	EN 55022:1998, Class A, 30 MHz to 5 GHz	Radiated Emissions
	EN 55022:1998, Class A, 150 kHz to 30 MHz	Conducted Emissions
	CISPR 24:1997/EN 55024:1998	Immunity for ITE
	EN 61000-4-2:1995, 8kV CD / 15kV AD	ESD
	EN 61000-4-3:1996,100kHz-1GHz, 10V/m, 1kHz AM	Radiated Immunity
	ENV 50204:1995, 900MHz/1.89GHz, PM, 10 V/m	Radiated Immunity
	EN 61000-4-4:1995, 1kV Power line, 0.5kV signal cables	EFT
	EN 61000-4-5:1995, 2kV CM, 1kV DM	Surge
	EN 61000-4-6:1996, 150kHz - 400MHz, $3V_{rms}$, 1kHz AM	Conducted Immunity
	EN 61000-4-8:1993, 3 A/m, 50Hz	Magnetic Immunity
	EN 61000-4-11:1994, $11V_{rms}$ (10ms), $161V_{rms}$ (0.5s), $11 V_{rms}$ (5s)	Voltage Dips & Interrupts
	EN61000-3-2; '95 +A14	Power line Harmonics
	EN61000-3-3; '95	Voltage Flicker

Supplementary Information:
The product as stated above complies with the requirements of the Low Voltage Directive 73/23/EEC, and the EMC Directive 89/336/EEC, as amended by 93/68/EEC.

May 31, 2001
Date

Cecil Clayton
by: Cecil Clayton
Hewlett-Packard Company
Product Regulations Manager

European Contact: Your Local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department HQ-TRE / Standards Europe, Herrenberger Strasse 130, D-71034 Boeblingen, Germany (FAX +49-7031-14-3143)

1 of 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls - Nº 781
Doc.

Figure 10 Superdome Declaration of Conformity Page 2

FCC Regulations (USA Only)

The Federal Communications Commission (in 47 CFR Part 15) has specified that the following notice be brought to the attention of the users of this product.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance (Hewlett-Packard) could result in the equipment being non-compliant with the FCC Class A requirements and void the user's authority to operate the equipment.

Additional International Approvals

AS/NZS 3548:1995 C-Tick & Supplier Code (N279)	Australia/New Zealand
CSA C22.2 No. 950-95	Canada
ICES-003 Issue 3	Canada
GB4943-1995	China
GB9254-1988	China
VCCI Class A	Japan
MIC No. 1996-18, Class A	Korean
BSMI, CNS-13438 (1994(Rev. 5/97)	Taiwan

IEC 60950 Evaluated National Differences for the following countries and areas.

CENELEC, AT= Austria, AU= Australia, BE= Belgium, CA= Canada, CH= Switzerland, CN= China, CZ= Czech Republic, DE= Germany, DK= Denmark, ES= Spain, FI= Finland, FR= France, GB= United Kingdom, GR= Greece, HU= Hungary, IE= Ireland, IL= Israel, IN= India, IT= Italy, JP= Japan, KR= Republic of Korea, NL= The Netherlands, NO= Norway, PL= Poland, RU= Russia, SE= Sweden, SG= Singapore, SI= Slovenia, SK= Slovakia, TR= Turkey, UA= Ukraine, US= United States, ZA= South Africa

Figure 9 Superdome Declaration of Conformity Page 1

DECLARATION OF CONFORMITY

according to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name:	Hewlett-Packard Company
Address:	3000 Waterview Parkway Richardson, TX 75080, USA

declares that the product

Product Name:	SUPERDOME (HP High Performance SMP Server)
Model Number(s):	SPP5 [Marketing nomenclature: Model 16, SD16000, Model 32, SD32000 Model 64, SD64000]
Base Product Number(s):	A5200A, A5201A, A5202A, A6115A, A6445A, A6862A
Product Option(s):	All

conforms to the following Product Specifications:

Safety: IEC 60950:1991 + A1 + A2 + A3 + A4 (with national differences for the countries & areas listed on page 21
EN 60950:1992 + A1 + A2 + A3 + A4 + A11
UL 1950, Third Edition, CAN/CSA C22.2 No. 950-95, Third Edition

EMC:	CISPR 22:1997 / EN 55022: 1998 Class A	
	EN 55022:1998, Class A, 30 MHz to 5.56 GHz	Radiated Emissions
	EN 55022:1998, Class A, 150 kHz to 30 MHz	Conducted Emissions
	EN 55024:1998	Immunity for ITE
	EN 61000-4-2:1995, 8kV CD / 15kV AD	ESD
	EN 61000-4-3:1996, 100kHz-30MHz, 10 V/m, 1kHz AM 30MHz-80MHz, 3V/m, 1kHz AM 80MHz-1GHz, 10V/m, 1kHz AM	Radiated Immunity
	ENV 50204:1995, 900MHz, 1.89GHz, PM, 10 V/m	Radiated Immunity
	EN 61000-4-4:1995, 1kV Power line, 0.5kV signal cables	EFT
	EN 61000-4-5:1995, 2kV CM, 1kV DM	Surge
	EN 61000-4-6:1996, .150MHz - 400MHz, 3 V_{rms}, 1kHz AM	Conducted Immunity
	EN 61000-4-8:1993, 3 A/m, 50Hz	Magnetic Immunity
	EN 61000-4-11:1994, 1 V_{rms} (10ms), 161 V_{rms} (0.5s), 11 V_{rms} (5s)	Voltage Dips & Interrupts

Supplementary Information:
The product as stated above complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC, as amended by 93/68/EEC

April 25, 2002
Date

Cecil Clayton

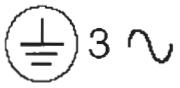
by Cecil Clayton
Hewlett-Packard Company
Product Regulations Manager

For [illegible] Hewlett-Packard GmbH, Department HQ-TRE, Standards Europe, Herrenberger Strasse 130, D-71034 Boeblingen, Germany (FAX: +49-7031-14-3143)

RQS nº 03/2005 - CN
CPMI - CORREIOS
1982
Fls. Nº
3698
Doc.

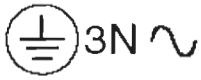
International Symbols (IEC335-1)

Figure 7 Four Wire Connection



Protective earth, 3-phase AC

Figure 8 Five Wire Connection



Protective earth, 3-phase AC plus neutral return

Associated Documents

The following documents provide more details on the topics presented in this manual:

- *Standard for the Protection of Electronic Computer Data Processing Equipment*, (NFPA75) National Fire Protection Association
- EIA Standard RS-232-C, Electronic Industries Association
- *Electrostatic Discharge Failures of Semiconductor Devices*, Unger, B.A. 1981, Bell Laboratories
- IEC 60950, EN 60950, UL 60950, CSA 22.2 No. 950 *Standards for Safety of Information Technology Equipment*
- IEC 60417, IEC 335-1, ISO 3864, IEC 617-2 International Symbols

ECT
Paula
CPL - AC

WARNING **If the system has two PDCA installed, ensure that power is removed from both PDCA before removing fuses.**

Fuse Warnings

Superdome Only:

WARNING **Disconnect power before changing fuse.**

CAUTION For continued protection against risk of fire, replace fuses only with same type and rating.

Lithium Battery Caution

WARNING **Observe the correct polarity when changing the lithium battery. There is a danger of explosion if battery is installed incorrectly.**

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions and local disposal requirements.

IMPORTANT Switzerland: Annex 4.10 of SR 814.013 applies to batteries.

Australian C-Tick Label

Figure 6

C N279

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 783
Doc.

Table 4 Wall Disconnect Device Circuit Breaker Specification (Continued)

Circuit Interruption	Simultaneous trip of all poles
Ground	The protective earth (PE) ground wire is not switched

WARNING **Provide a disconnect device to protect against abnormal hazards.**

Systems configured with a full complement of cells, memory, and I/O and connected to a 5-wire source must have a maximum 24A 3-phase with neutral (4-pole) circuit breaker installed as part of the building installation.

Systems configured with a full complement of cells, memory, and I/O and connected to a 4-wire source must have a maximum 44A 3-phase (3-pole) circuit breaker installed as part of the building installation.

CAUTION Refer to Table E-1 on page 104 to select the appropriate size circuit breaker for systems configured without a full complement of cells, memory, and I/O.

Table E-1 on page 104 shows Superdome power requirements by configuration (i.e. number of cell boards, amount of memory per cell, and number of I/O chassis). This requirement applies to 32-way-capable systems with PA8600 or PA8700 processors.

There are two columns of power numbers (Watts). The Power Breaker column shows the power used to size the wall breaker at the installation site. The Typical Power column shows typical power. Typical power numbers are for PA8600 systems and may be used to assess average utility cost of cooling and electrical power. Expect these typical numbers to be about 18% less for PA8700 systems.

CAUTION For supply connections, use wires suitable for at least 105 °C.

Utillser des fils convenant á une température de 105 °C pour les connexions d'allmenation.

Network Connected Equipment The installation must provide a ground connection for the network equipment.

CAUTION Sweden: Apparaten skall anslutas till jordat uttang när deb abskuts till ett nätverk.

IOX Multiple Power Sources and Cords

This equipment may be configured with dual-input line sources. Hazardous voltages and energy may be present even after the removal of a single input source. Trained service personnel must follow the guidelines stipulated in the *Service Guidelines* section of the Superdome EPSS.

IOX Only:

WARNING **Remove both input power sources before replacing an internal fuse.**

Install a PE (protective earthing) conductor that is identical in size, insulation material, and thickness to the branch-circuit supply conductors. The PE conductor insulation must be green with yellow stripes. The earthing conductor is to be connected from the unit to the building installation earth or, if supplied by a separately derived system, at the supply transformer or motor-generator set grounding point.

WARNING NORDIC Class 1 Equipment

Denmark: Før tilslutning af de øvrige ledere, se medfølgende installationsvejledning.

WARNING NORDIC Class 1 Equipment

Sweden: Apparaten skall anslutas till jordat uttag, när den ansluts till ett nätverk.

Recommended Wire Sizes Table 3 shows the wire size requirements for conductors in power supply cords (Extracted from IEC 60950, Table 11).

NOTE Specific countries require a derating factor for the wire size when running multiple conductors in the same power cord. It is Hewlett-Packards recommendation to use only power cord conductors sized for this derating factor.

Table 3 Recommended Wire Sizes

Current	Wire Size	Derating Factor
0-25 Amps	2.5 mm (14 AWG)	4 mm (12 AWG)
25-32 Amps	4 mm (12 AWG)	6 mm (10 AWG)
32-40 Amps	6 mm (10 AWG)	10 mm (8 AWG)
40-63 Amps	10 mm (8 AWG)	16 mm (6 AWG)
63-80 Amps	16 mm (6 AWG)	25mm (4 AWG)

Disconnect Devices Disconnect devices or circuit breakers must be used to protect the system against abnormal hazards. Table 4 details the circuit breaker specifications.

Table 4 Wall Disconnect Device Circuit Breaker Specification

Agency approvals:	UL, CSA, VDE
Interrupt capacity	5,000A minimum
Breaker type	Magnetic trip
Voltage rating	250V minimum 3-pole+PE, 420V minimum 4-pole+PE
Input Source	3 pole + PE or 4-pole + PE

BSMI (Taiwan Areas)

This product is fully compliant to CNS 13438 (CISPR 22: 1993) Class A. The EMC label is in the form shown in Figure 4. The eight # signs represent an eight-character, alpha-number string.

Figure 4

檢磁 ########

Figure 5

Acoustics (Germany)

Acoustic Noise (A-weighted Sound Pressure Level LpA) measured at the bystander position, normal operation, to ISO 7779: LpA = 65.1 dB.

Geräuschemission (Deutschland)

Lärmangabe (Schalldruckpegel LpA) gemessen am fiktiven Arbeitsplatz bei normalem Betrieb nach DIN 45635, Teil 19: LpA = 65.1 dB.

IT Power System

This product has not been evaluated for connection to an IT power system (an AC distribution system having no direct connection to earth according to IEC 60950).

TT, TN-C, and TN-C-S Power Systems

These products should not be connected to power systems that switch open the return lead when the return lead also functions as the protective earth (PE). A separate PE ground wire must be connected to the equipment at the designated PE terminal tie point.

High Leakage Current

WARNING **High leakage current. Ground (earth) connection essential before connecting the supply.**

Installation Conditions

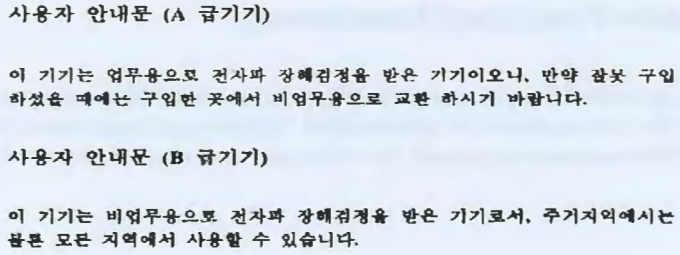
See installation instructions before connecting this equipment to the input supply.

Voir la notice d'installation avant de raccorder au réseau.

WARNING **Please note the following conditions of installation:**

- CCCC: registration number

Figure 3 Korean RFI



사용자 안내문 (A 급기기)

이 기기는 업무용으로 전자파 장해검정을 받은 기기이오니, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환 하시기 바랍니다.

사용자 안내문 (B 급기기)

이 기기는 비업무용으로 전자파 장해검정을 받은 기기로서, 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다.

Translation

Class A Equipment:

Please note that this equipment has been approved for business purpose with regards to electromagnetic interference, if purchased un error for use in residential area, you may wish to exchange the equipment where you purchase it.

Class B Equipment:

Please note that this equipment has been approved for non-business with regards to electromagnetic interference. So, this equipment can be allowed to use all area as well as residential area.

European Union RFI Statement

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Canada RFI Statement

This Class A digital apparatus complies with Canadian ICES-003.

Notice relative aux interférences radioélectriques (Canada)

Cet appareil numéric de la classe A est conforme à la norme NMB-003 du Canada.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 785
Doc.

The user is cautioned that changes or modifications not expressly approved by Hewlett-Packard could result in the equipment being noncompliant with FCC Class A requirements and void the user's authority to operated the equipment.

Japanese Radio Frequency Interference VCCI

This equipment is in the Class A category information technology equipment based on the rules of Voluntary Control Council For Interference by Information Technology Equipment (VCCI). When used in a residential area, radio interference may be caused. In this case, user may be required to take appropriate corrective actions.

Figure 1

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean RFI Statement

1. Equipment Name (Model Name):
2. Certification No:
3. Name of Certification Recipient:
4. Date of Manufacture:
5. Manufacturer/Nation:

Figure 2

MIC

1. 명 칭 (모델명) :
2. 인 증 번 호 :
3. 인 증 자 상 호 : 한국휴렛팩커드(주)
4. 제 조 년 월 일 : 별도표기
5. 제조자/제조국 :

Certification Number: E - AAAAA - BB - CCCC

- E: EMC registration
- AAAAA: equipment codes (RRL notice, 2000.10.26)
- BB: certification year
- CCCC: registration number

- E: EMC registration
- AAAAA: equipment codes (RRL notice, 2000.10.26)
- BB: certification year

E C T
CPL - AC

WARNING **Use care when lifting a cell board. Each cell board can weigh as much as 48 pounds (22kg).**

WARNING **Use care when working with hazardous voltages. This equipment may be configured with dual input line sources. Hazardous voltages and energy maybe present even after the removal of a single input source. Trained service personnel must follow the service guidelines.**

WARNING **Do not stand in front of the equipment as it is rolled off the pallet onto the ramps. When removing the equipment from the shipping pallet, follow the guidelines specified in the Installation Procedures section of the appropriate equipment guides (Superdome or I/O Expansion Cabinet).**

WARNING **Do not attempt to move the Superdome cabinet, either packed or unpacked, up or down an incline of more than 15 degrees.**

IOX Only:

WARNING **Attach stabilizer feet to both front and back before extending the equipment drawers. Failure to attach the stabilizer feet may result in a tip hazard.**

IOX Only:

WARNING **Observe pinch hazard areas. Keep fingers away from closing parts.**

USA Radio Frequency Interference FCC Notice

The Federal Communications Commission (in 47 CFR Part 15 subpart B) has specified that the following notice be brought to the attention of the users of this product.

NOTE This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 186
Doc. 3698

Safety and Regulatory Information

For your protection, this product has been tested to various national and international regulations and standards. The scope of this regulatory testing includes electrical/mechanical safety, radio frequency interference, acoustics, and know hazardous materials.Where applicable, approvals obtained from third-party test agencies are shown on the product label.

Notational Conventions

WARNING **Warnings highlight procedures or information necessary to avoid injury to personnel. The warning should tell the reader exactly what will result from what actions and how to avoid them.**

CAUTION A caution highlights procedures or information necessary to avoid damage to equipment, damage to software, loss of data, or invalid test results.

NOTE A note highlights supplemental information.

Acronyms

Table 2 lists acronyms used in this document.

Table 2 Acronyms

Acronym	Definition
PE	Protective earth
Class 1	Grounded equipment
PDCA	Power Distribution Controller Assembly
EPSS	Electronic Performance Support Service

Safety in Material Handling

WARNING **Do not lift the cabinet manually. To avoid physical injury you must use a mechanical lifting device.**

Revision History

Table 1 Revisions After May 2001

Revision	Part Number	Release Date	Description
Eighth		June 2002	Added recommendations for the in-line connector and the wall panel receptacle that are supplied by the end user (customer). These parts are not provided by H.P. due to the extensive options available for the cusomter's building wiring infrastructure. Added miscellaneous updates and corrections.
Seventh	A5201-10023	November 2001	Added new PDCA options.
Sixth	A5201-10016	August 2001	Updated for Caribe. Update safety and regulatory information. Changed power, circuit breaker, and wiring infomation. Added ramp angle note.
Fifth	A5201-10013	July 2001	Added Safety and Regulatory section. Added info on lower breaker value usage, pay-per-use and iCOD modem support, and general corrections per edits.
Fourth	A5201-10011	May 2001	Added IOX information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
787
Fls. Nº
Doc.

Preface

ECT 9851 Paula CPL.

Contents

3. Facility Guidelines

Facility Characteristics 57
Floor Loading 57
Windows 59
Space Requirements. 60
Delivery Space Requirements 60
Operational Space Requirements 60
Floor Plan Grid 60
Equipment Footprint Templates 61

4. Pre-Installation Survey

Pre-Installation Survey Content 65
Typical Installation Schedule 66
Site Inspection 67
Delivery Survey 71

A. System Weights

Weight 76

B. Conversion Factors

C. Templates

Equipment Footprint Templates 85
Computer Room Layout Plan 86

D. Superdome LAN Interconnect Diagram

E. Superdome Configurations

RQS nº 03/2005 - CN
CPMI - CORREIOS
788
Fls: Nº
3698
Doc.

Contents

1. System Specifications

General . . . 3
Server System . . . 4
Basic System Building Blocks . . . 4
Server Cabinet . . . 7
Upgrading Superdomes and Server Systems . . . 9
Upgrading the Server . . . 9
Upgrading the System . . . 9
Dimensions and Weights . . . 10
Component Dimensions . . . 10
Component Weights . . . 11
Shipping Dimensions and Weights . . .
Electrical Specifications . . . 13
Grounding . . . 13
Circuit Breaker . . . 13
Input Power Options . . . 14
Power Cords . . . 19
System Power Requirements . . . 28
Component Power Requirements . . . 28
I/O Expansion Cabinet Power Requirements . . . 29
I/O Expansion Cabinet Power Cords . . . 29
Peripheral Cabinet Power Requirements . . . 29
Support Management Station Power Requirements . . . 30
Environmental Requirements . . . 31
Temperature and Humidity Specifications . . . 31
Power Dissipation . . . 31
Acoustic Noise Specification . . . 32
Air Flow . . . 32

2. Electrical and Environmental Guidelines

Electrical Factors . . . 39
Computer Room Safety . . . 39
Power Quality . . . 40
Distribution Hardware . . . 41
Grounding Systems . . . 41
System Installation Guidelines . . . 42
Environmental Elements . . . 44
Computer Room Preparation . . . 44
Cooling Requirements . . . 44
Humidity Level . . . 50
Air Conditioning Ducts . . . 51
Dust and Pollution Control . . . 51
Zinc Particulate Contamination . . . 52
Electrostatic Discharge (ESD) Prevention . . . 52
Acoustics . . . 53

ECT
8853
Paula
CPL - AC

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY 3000 Hanover Street Palo Alto, California 94304 U.S.A.

Copyright Notices. ©copyright 1983-2002 Hewlett-Packard Company, all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 789
Doc. 3698

Superdome Site Preparation Guide

HP 9000 Systems

Eighth Edition

Manufacturing Part Number: A5201-10024
80602

USA

© Copyright 2002

Eighth Edition

June 2002

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 790
Doc. 3698

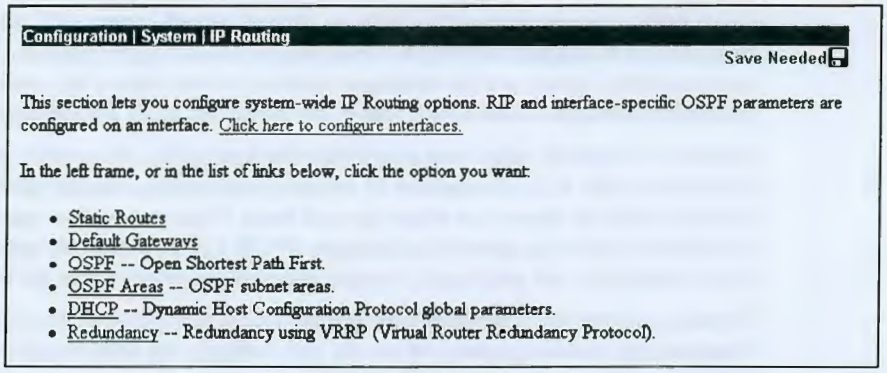
Configuration | System | IP Routing

This section of the Manager lets you configure system-wide IP routing parameters:

- Static Routes: Manually configured routing tables.
- Default Gateways: Routes for otherwise unrouted traffic.
- OSPF: Open Shortest Path First routing protocol.
- OSPF Areas: Subnet areas within the OSPF domain.
- DHCP: Dynamic Host Configuration Protocol global parameters.
- Redundancy: Virtual Router Redundancy Protocol parameters.

You configure RIP and interface-specific OSPF parameters on the network interfaces; click the highlighted link to go to the Configuration | Interfaces screen.

Figure 8-1 Configuration / System / IP Routing Screen



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 791
78-13273-01
Doc.

CHAPTER 8

IP Routing

In a typical installation, the VPN Concentrator is connected to the public network through an external router, which routes data traffic between networks, and it might also be connected to the private network through a router.

The VPN Concentrator itself includes an IP routing subsystem with static routing, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First) functions. RIP and OSPF are routing protocols that routers use for messages to other routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic.

Once the IP routing subsystem establishes the data paths, the routing itself occurs at wire speed. The subsystem looks at the destination IP address in all packets coming through the VPN Concentrator, even tunneled ones, to determine where to send them. If the packets are encrypted, it sends them to the appropriate tunneling protocol subsystem (PPTP, L2TP, IPSec) for processing and subsequent routing. If the packets are not encrypted, it routes them in accordance with the configured IP routing parameters.

To route packets, the subsystem uses learned routes first (learned from RIP and OSPF), then static routes, then uses the default gateway. If you do not configure the default gateway, the subsystem drops packets that it cannot otherwise route. The VPN Concentrator also provides a tunnel default gateway, which is a separate default gateway for tunneled traffic only.

You configure static routes, the default gateways, and system-wide OSPF parameters in this section. This section also includes the system-wide DHCP (Dynamic Host Configuration Protocol) parameters. You configure RIP and interface-specific OSPF parameters on the network interfaces; see Configuration Interfaces.

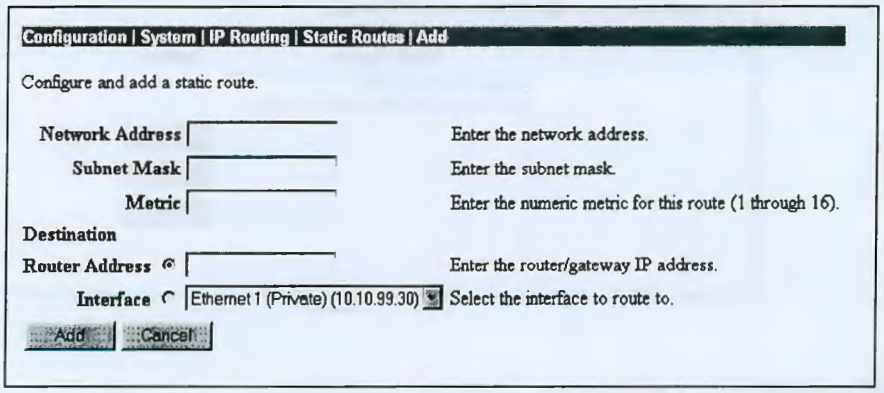
This section of the Manager also lets you configure VPN Concentrator redundancy using VRRP (Virtual Router Redundancy Protocol). This feature applies to installations of two or more VPN Concentrators in a parallel, redundant configuration. It provides automatic switchover to a backup system in case the primary system is out of service, thus ensuring user access to the VPN. This feature supports user access via IPSec LAN-to-LAN connections, IPSec client (single-user remote-access) connections, and PPTP client connections.

Configuration | System | IP Routing | Static Routes | Add or Modify

These Manager screens let you:

- Add: Configure and add a new static, or manual, route to the IP routing table.
- Modify: Modify the parameters for a configured static route.

Figure 8-3 Configuration / System / IP Routing / Static Routes / Add or Modify Screen



Network Address

Enter the destination network IP address to which this static route applies. Packets with this destination address will be sent to the destination you enter. Used dotted decimal notation, for example: 192.168.12.0.

Subnet Mask

Enter the subnet mask for the destination network IP address. Use dotted decimal notation, for example: 255.255.255.0. The subnet mask indicates which part of the IP address represents the network and which part represents hosts. The router subsystem looks at only the network part.

The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.0 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed here, since that would resolve to the equivalent of a default gateway.

Metric

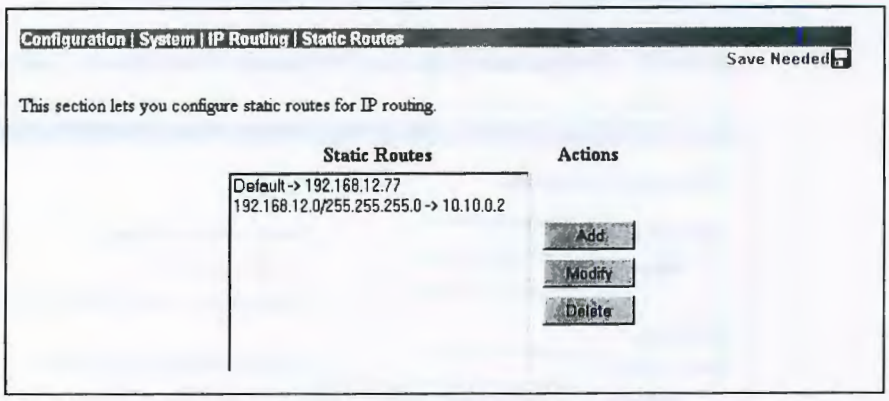
Enter the metric, or cost, for this route. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 792
Doc.

Configuration | System | IP Routing | Static Routes

This section of the Manager lets you configure static routes for IP routing. You usually configure static routes for private networks that cannot be learned via RIP or OSPF.

Figure 8-2 Configuration / System / IP Routing / Static Routes Screen



Static Routes

The Static Routes list shows manual IP routes that have been configured. The format is *[destination network address/subnet mask -> outbound destination]*, for example: 192.168.12.0/255.255.255.0 -> 10.10.0.2. If you have configured the default gateway, it appears first in the list as Default -> default router address. If no static routes have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new static route, click **Add**. The Manager opens the Configuration | System | IP Routing | Static Routes | Add screen.

To modify a configured static route, select the route from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | Static Routes | Modify screen. If you select the default gateway, the Manager opens the Configuration | System | IP Routing | Default Gateways screen.

To delete a configured static route, select the route from the list and click **Delete**.

Note There is no confirmation and no undo.

The Manager refreshes the screen and shows the remaining static routes in the list. You cannot delete the default gateways here; to do so, see the Configuration | System | IP Routing | Default Gateways screen.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

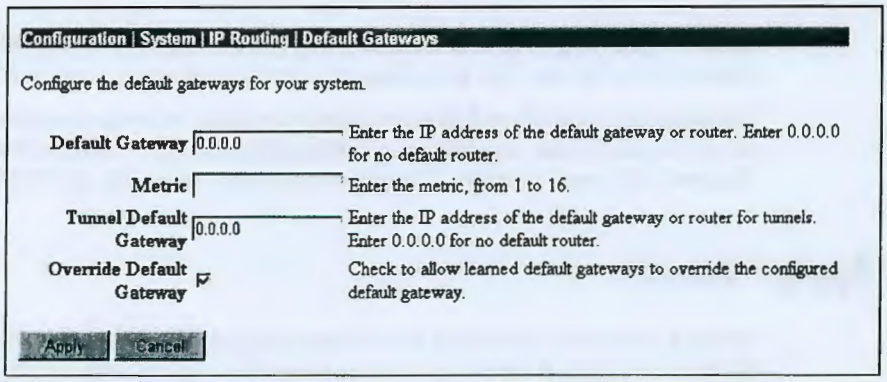
Configuration | System | IP Routing | Default Gateways

This screen lets you configure the default gateway for IP routing, and configure the tunnel default gateway for tunneled traffic. You use this same screen both to initially configure and to change default gateways. You can also configure the default gateway on the Configuration | Quick | System Info screen.

The IP routing subsystem routes data packets first using learned routes, then static routes, then the default gateway. If you do not specify a default gateway, the system drops packets it cannot otherwise route.

For tunneled data, if the system does not know a destination address, it tries to route the packet to the tunnel default gateway first. If that route is not configured, it uses the regular default gateway.

Figure 8-4 Configuration / System / IP Routing / Default Gateways Screen



Default Gateway

Enter the IP address of the default gateway or router. Use dotted decimal notation, for example: 192.168.12.77. This address must *not* be the same as the IP address configured on any VPN Concentrator interface. If you do not use a default gateway, enter 0.0.0.0 (the default entry).

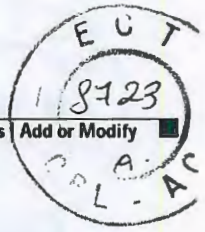
To delete a configured default gateway, enter `0.0.0.0`.

The default gateway must be reachable from a VPN Concentrator interface, and it is usually on the public network. The Manager displays a warning screen if you enter an IP address that is not on one of its interface networks, and it displays a dialog box if you enter an IP address that is not on the public network.

Metric

Enter the metric, or cost, for the route to the default gateway. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if this route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 793
Doc.



Destination

Click a radio button to choose the outbound destination for these packets. You can choose only one destination: either a specific router/gateway, or a VPN Concentrator interface.

Router Address

Enter the IP address of the specific router or gateway to which to route these packets; that is, the IP address of the next hop between the VPN Concentrator and the ultimate destination of the packet. Use dotted decimal notation, for example: 10.10.0.2.

Interface

Click the **Interface** drop-down menu button and choose a configured VPN Concentrator interface as the outbound destination. The menu lists all interfaces that have been configured.

For example, in a LAN-to-LAN configuration where remote-access clients are assigned IP addresses that are not on the private network, you could configure a static route with those addresses outbound to the Ethernet 1 (Private) interface. The clients could then access the peer VPN Concentrator and its networks.

Add or Apply / Cancel

To add a new static route to the list of configured routes, click **Add**. Or to apply your changes to a static route, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | IP Routing | Static Routes screen. Any new route appears at the bottom of the Static Routes list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | Static Routes screen, and the Static Routes list is unchanged.

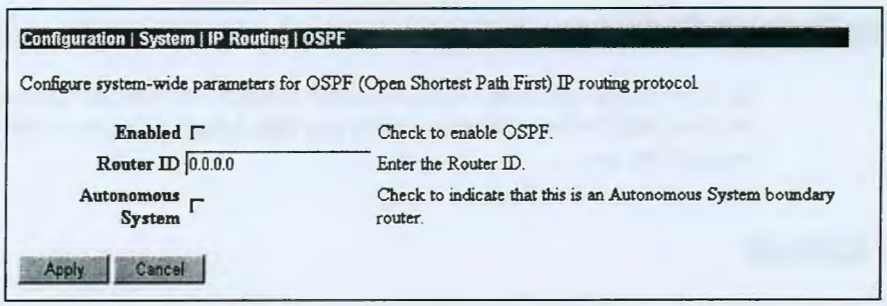
Configuration | System | IP Routing | OSPF

This screen lets you configure system-wide parameters for the OSPF (Open Shortest Path First) routing protocol. You must also configure interface-specific OSPF parameters on the Configuration | Interfaces screens.

OSPF is a protocol that the IP routing subsystem uses for messages to other OSPF routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic. The VPN Concentrator supports OSPF version 2 (RFC 2328).

The complete private network is called an OSPF Autonomous System (AS), or domain. The subnets within the AS are called areas. You configure OSPF areas on the Configuration | System | IP Routing | OSPF Areas screens.

Figure 8-5 Configuration | System | IP Routing | OSPF Screen



Enabled

To enable the VPN Concentrator OSPF router, check the **Enabled** check box. (By default it is unchecked.) You must also enter a Router ID. You must check this box for OSPF to work on any interface that uses it.

To change a configured Router ID, you must disable OSPF here.

To enable OSPF routing on an interface, you must also configure and enable OSPF on the appropriate Configuration | Interfaces screen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 794
Doc.

Tunnel Default Gateway

Enter the IP address of the default gateway for tunneled data. Use dotted decimal notation, for example: 10.10.0.2. If you do not use a tunnel default gateway, enter `0.0.0.0` (the default entry).

To delete a configured tunnel default gateway, enter `0.0.0.0`.

This gateway is often a firewall in parallel with the VPN Concentrator and between the public and private networks. The tunnel default gateway applies to all tunneled traffic, including IPSec LAN-to-LAN traffic.

Note If you use an external device instead of the VPN Concentrator for NAT (Network Address Translation), you must configure the tunnel default gateway.

Override Default Gateway

To allow default gateways learned via RIP or OSPF to override the configured default gateway, check the **Override Default Gateway** check box (the default). To always use the configured default gateway, uncheck the box.

Apply / Cancel

To apply the settings for default gateways, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen. If you configure a Default Gateway, it also appears in the Static Routes list on the Configuration | System | IP Routing | Static Routes screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

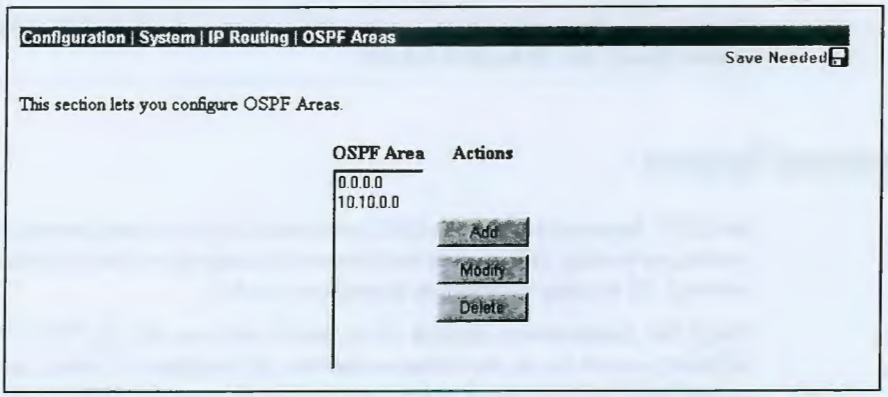
To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Ro g screen.

Configuration | System | IP Routing | OSPF Areas

This section of the Manager lets you configure OSPF areas, which are the subnets within an OSPF Autonomous System or domain. You should configure entries for all areas connected to this VPN Concentrator OSPF router.

You can also identify an OSPF area on a VPN Concentrator network interface (see Configuration | Interfaces). Those area identifiers appear in the OSPF Area list on this screen.

Figure 8-6 Configuration / System / IP Routing / OSPF Areas Screen



OSPF Area

The OSPF Area list shows identifiers for all areas that are connected to this VPN Concentrator OSPF router. The format is the same as a dotted decimal IP address, for example: 10.10.0.0. The default entry is 0.0.0.0. This entry identifies a special area known as the backbone that contains all area border routers, which are the routers connected to multiple areas.

Add / Modify / Delete

To configure and add a new OSPF area, click **Add**. The Manager opens the Configuration | System | IP Routing | OSPF Areas | Add screen.

To modify a configured OSPF area, select the area from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | OSPF Areas | Modify screen.

To delete a configured OSPF area, select the area from the list and click **Delete**.

Note There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the OSPF Area list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 795
Doc.

Router ID

The router ID uniquely identifies the VPN Concentrator OSPF router to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network.

Enter the router ID in the field. Use dotted decimal IP address format, for example: 10.10.4.6. The default entry is 0.0.0.0 (no router configured). If you enable the OSPF router, you must enter an ID.

Note Once you configure and apply a router ID, you must disable OSPF before you can change it. You cannot change the ID back to 0.0.0.0.

Autonomous System

An OSPF Autonomous System (AS), or domain, is a complete internal network. An AS boundary router exchanges routing information with routers belonging to other Autonomous Systems, and advertises external AS routing information throughout its AS.

Check the **Autonomous System** check box to indicate that the VPN Concentrator OSPF router is the boundary router for an Autonomous System. If you check this box, the VPN Concentrator also redistributes RIP and static routes into the OSPF areas. By default, the box is unchecked.

Apply / Cancel

To apply your OSPF settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

External LSA Import

Click the **External LSA Import** drop-down menu button and choose whether to bring in LSAs from neighboring Autonomous Systems. LSAs describe the state of the AS router's interfaces and routing paths. Importing those LSAs builds a more complete link-state database, but it requires more processing. The choices are:

- External = Yes, import LSAs from neighboring ASs (the default).
- No External = No, do not import external LSAs.

Add or Apply / Cancel

To add this OSPF area to the list of configured areas, click **Add**. Or to apply your changes to this OSPF area, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | IP Routing | OSPF Areas screen. Any new entry appears at the bottom of the OSPF Area list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | OSPF Areas screen, and the OSPF Area list is unchanged.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 796
Doc.

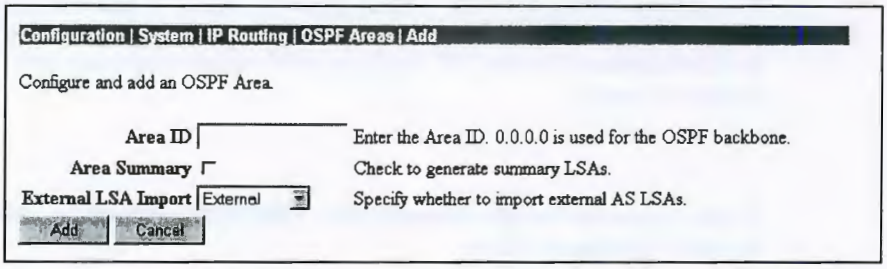
Configuration | System | IP Routing | OSPF Areas | Add or Modify

These Manager screens let you:

- Add: Configure and add an OSPF area.
- Modify: Modify parameters for a configured OSPF area.

Note Once you have configured an OSPF Area, you cannot modify its ID. To change an area ID, delete the existing area and add a new one.

Figure 8-7 Configuration / System / IP Routing / OSPF Areas / Add or Modify Screen



Area ID

- Add: Enter the area ID in the field. Use IP address dotted decimal notation, for example: 10.10.0.0. The default entry is 0.0.0.0, the backbone.
- Modify: Once you have configured an area ID, you cannot change it. See preceding note.

The Area ID identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. The 0.0.0.0 area ID identifies a special area—the backbone—that contains all area border routers.

Area Summary

Check the **Area Summary** check box to have the OSPF router generate and propagate summary LSAs (Link-State Advertisements) into OSPF stub areas. LSAs describe the state of the router's interfaces and routing paths. Stub areas contain only final-destination hosts and do not pass traffic through to other areas. Sending LSAs to them is usually not necessary. By default this box is unchecked.

Listen Port

Enter the UDP port number on which DHCP server response messages are accepted. The default is 67, which is the well-known port. *To ensure proper communication with DHCP servers, we strongly recommend that you not change this default.*

Timeout Period

Enter the initial time in seconds to wait for a response to a DHCP request before sending the request to the next configured DHCP server. The minimum time is 1 second. The default time is 2 seconds. The maximum time is 10 seconds. This time doubles with each cycle through the list of configured DHCP servers.

Apply / Cancel

To apply the settings for DHCP parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

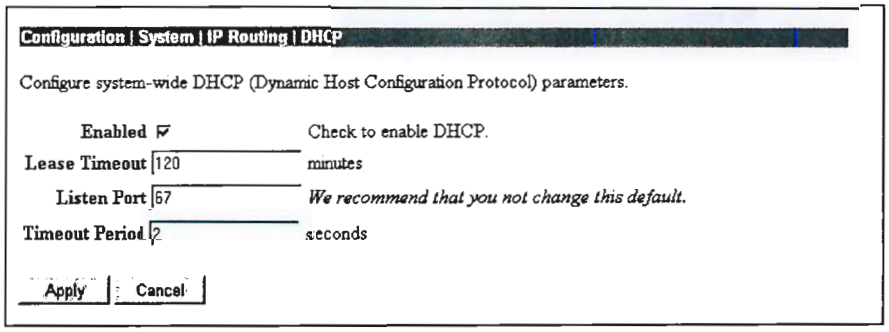
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 797
Doc.

Configuration | System | IP Routing | DHCP

This screen lets you configure DHCP (Dynamic Host Configuration Protocol) parameters that apply to DHCP functions within the VPN Concentrator. You can use external DHCP servers to assign IP addresses to clients as a VPN tunnel is established.

If you check the Use DHCP check box on the Configuration | System | Address Management | Assignment screen, you must configure at least one DHCP server on the Configuration | System | Servers | DHCP screens. You configure global DHCP parameters here.

Figure 8-8 Configuration / System / IP Routing / DHCP Screen



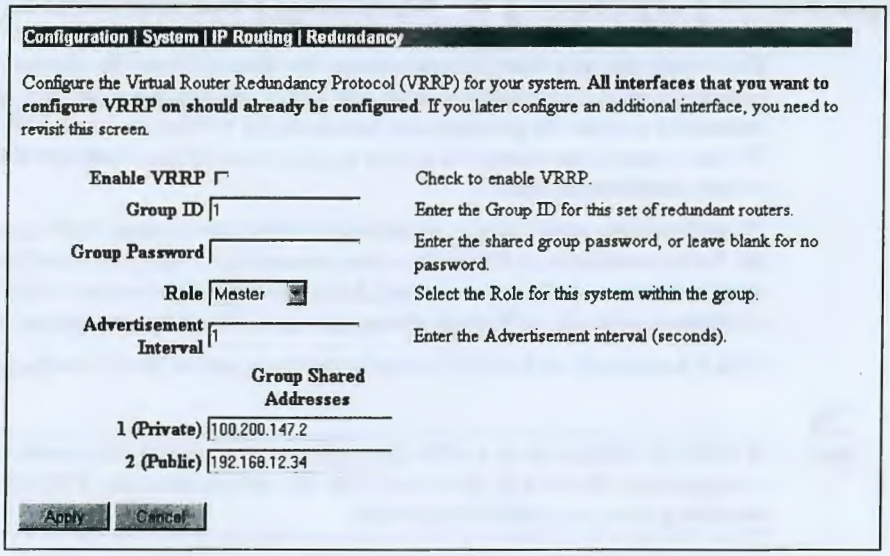
Enabled

Check the **Enabled** check box to enable DHCP functions within the VPN Concentrator. The box is checked by default. To use DHCP address assignment, you must enable DHCP functions here.

Lease Timeout

Enter the timeout in minutes for addresses that are obtained from a DHCP server. The minimum timeout is 5 minutes. The default is 120 minutes. The maximum is 500000 minutes. DHCP serves "lease" IP addresses for this period of time. Before the lease expires, the VPN Concentrator asks to renew it on behalf of the client. If for some reason the lease is not renewed, the connection terminates when the lease expires. The DHCP server's lease period takes precedence over this setting.

Figure 8-9 Configuration / System / IP Routing / Redundancy Screen



Enable VRRP

Check the **Enable VRRP** check box to enable VRRP functions. The box is unchecked by default.

Group ID

Enter a number that uniquely identifies this group of redundant VPN Concentrators. This number must be the same on all systems in this group. Use a number from 1 (default) to 255. Since there is rarely more than one virtual group on a LAN, we suggest you accept the default.

Group Password

Enter a password for additional security in identifying this group of redundant VPN Concentrators. The maximum password length is 8 characters. The Manager shows your entry in clear text, and VRRP advertisements contain this password in clear text. This password must be the same on all systems in this group. Leave this field blank to use no password.

Role

Click the **Role** drop-down menu button and choose the role of this VPN Concentrator in this redundant group.

- Master = This is the Master system in this group (the default choice). Be sure to configure only one Master system in a group with a given Group ID.
- Backup 1 through Backup 5 = This is a Backup system in this group.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 798
Doc.

Configuration | System | IP Routing | Redundancy

This screen lets you configure parameters for Virtual Router Redundancy Protocol (VRRP), which manages automatic switchover from one VPN Concentrator to another in a redundant installation. Automatic switchover provides user access to the VPN even if one VPN Concentrator is out of service for some reason, for example a system crash, power failure, hardware failure, physical interface failure, system shutdown or reboot.

These functions apply only to installations where two or more VPN Concentrators are in parallel, with the Public interfaces of all systems on a common LAN and with the Private and/or External interfaces of all systems on different common LANs. One VPN Concentrator is the Master system, and the others are Backup systems. A Backup system acts as a virtual Master system when a switchover occurs.

VRRP works only on LAN (Ethernet) interfaces, not on WAN interfaces.

Note If VRRP is configured on a VPN Concentrator, you cannot also enable load balancing. In a VRRP configuration, the backup device remains idle unless the active VPN Concentrator fails. Load balancing does not permit idle devices.

This feature supports user access via IPSec LAN-to-LAN connections, IPSec client (single-user remote-access) connections, and PPTP client connections.

- For IPSec LAN-to-LAN connections, switchover is fully automatic. Users do not need to do anything.
- For single-user IPSec and PPTP connections, users are disconnected from the failing system but they can reconnect without changing any connection parameters.

Switchover typically occurs within 3 to 10 seconds.

Note Before configuring or enabling VRRP on this screen, you must configure all Ethernet interfaces that apply to your installation, on all redundant VPN Concentrators. See the Configuration | Interfaces screens.

Note You must also configure *identical* IPSec LAN-to-LAN parameters on the redundant VPN Concentrators. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screens.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 799
Doc.

Advertisement Interval

Enter the time interval in seconds between VRRP advertisements to other systems in this group. Only the Master system sends advertisements; this field is ignored on Backup systems while they remain Backup. The minimum interval is 1 second. The default interval is 1 second. The maximum is 255 seconds. Since a Backup system can become a Master system, we suggest you accept the default for all systems.

Group Shared Addresses

Enter the IP addresses that are treated as configured router addresses by all virtual routers in this group. The Manager displays fields only for the Ethernet interfaces that have been configured.

On the Master system, these entries are the IP addresses configured on its Ethernet interfaces, and the Manager supplies them by default.

On a Backup system, the fields are empty by default, and you must enter the same IP addresses as those on the *Master* system.

1 (Private)

The IP address for the Ethernet 1 (Private) interface shared by the virtual routers in this group.

2 (Public)

The IP address for the Ethernet 2 (Public) interface shared by the virtual routers in this group.

3 (External)

The IP address for the Ethernet 3 (External) interface shared by the virtual routers in this group.

Apply / Cancel

To apply the settings for VRRP, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Apêndice II

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 800
Doc.

Virtual Graphical Remote Console

Remote Insight Lights-Out Edition II delivers an embedded, hardware-based graphical remote console capability that provides virtual presence to servers in data center and remote sites, giving full control of remote server display, keyboard, and mouse. It seamlessly supports text and graphics modes, displaying all phases of remote server activities (shutting down, starting up, loading OS operation) and is OS independent (Microsoft® Windows®, NetWare, Red Hat & SuSE Linux). It works with a standard browser; no additional software is required on the remote server or client. The Remote Insight Lights-Out Edition II is based on a 200-MHz processor that now provides significantly faster performance in the Graphical Remote Console. The Remote Insight Lights-Out Edition II provides secure remote access to the host server by providing 128-bit encryption of the remote console data stream.

Virtual Power Button

Using the browser interface, Remote Insight Lights-Out Edition II can be used to remotely operate the power button of a host server. For example, if the host server is off, you can turn it on from Remote Insight Lights-Out Edition II. You can also power off and on the server in one step. A force server power off option is available for the Virtual Power Button in the event a momentary press is insufficient to power off a server with a failed operating system.

Virtual Media

The Virtual Floppy Drive allows an administrator to easily direct the remote host server to boot using an image of a floppy disk available anywhere on the network. The new USB-based Virtual Media feature extends the advantages by allowing an IT administrator to boot the remote server using a standard 1.44-MB diskette on the client machine, a CD on the client machine, or an image of the floppy from anywhere on the client's network. After the remote server has booted a USB-capable operating system (e.g., Windows 2000, Windows 2003 Server, or Red Hat Linux 7.2), the virtual floppy or CD is available as if it were a local USB device. The Virtual Media features save time and increase efficiency by eliminating the need to visit the remote server just to insert and use a diskette or CD. This feature allows administrators to carry out any of the following functions remotely:

- Run HP User Diagnostics on remote host servers
- Apply ROMPaq upgrades to remote servers
- Deploy an operating system on remote servers from a Virtual CD network drives
- Perform disaster recovery of failed operating systems
- Install applications on the remote server from a Virtual CD

(**NOTE**: Booting a remote server from USB-based Virtual Floppy and CD requires server hardware and ROM support of these USB media devices. Recent-shipping ProLiant servers include hardware support of USB media devices and need only a ROM update to support booting from a USB device. This support will be available via future ROM upgrades for USB-enabled servers and will be a standard feature of newer servers.)

Dedicated LAN Network Connectivity

The Remote Insight Lights-Out Edition II provides IT Administrators with a dedicated 10/100 Mbit network connection to the managed server. The board provides SNMP notification in case of server problems to the Central Site management station on a real-time basis, without needing to maintain separate telephone connections or modem sharing devices. If dial-up access is desired, the board can be used in combination with an external RAS or modem router gateway.

Browser Accessible

Remote Insight Lights-Out Edition II is accessible via Microsoft Internet Explorer 5.5(SP2) or later, Netscape Navigator 6. 2 or later, and Mozilla 1.0 or later. This allows easy access from anywhere, anytime to Remote Insight features to perform remote management tasks using a familiar user interface. The board has its own Web Server that is independent of the server operating system, and provides HTML pages to any browser to use the Remote Insight features.

Pocket PC Access

The Remote Insight Lights-Out Edition II provides support for wireless and dial-up access from the iPAQ Pocket PC handheld devices. The Remote Insight Lights-Out Edition II provides a special user interface when connecting from the iPAQ Pocket PC.

Auto-Configuration of IP Address via DNS/DHCP

Remote Insight lights-Out Edition II allows automatic network configuration and can be put to use straight out of the box. The board comes with a default name and DHCP client that leases an IP address when a DNS/DHCP server is on the network. Static IP and port configuration are also supported.

Directory Integration for User Management

The Remote Insight Lights-Out Edition II integrates with enterprise-class directory services to provide ***secure, scalable, and cost effective*** user management. Directory services, such as Microsoft Active Directory and Novell eDirectory, can be used to authorize directory users with assigned user roles to Remote Insight Lights-Out Edition II cards. An easy and reliable installation program is available to install a management console snap-in and extend customer's existing directory schema to enable directory support for the HP lights-out management products. A directory migration tool is available to automate the integration of existing HP lights-out management devices to directory services. The Remote Insight Lights-Out Edition II also supports up to 25 local user accounts with customizable access rights, each with individual login and password.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 801
Doc. 3698

Overview

MODELS

Remote Insight Lights-Out Edition II

227251-001

The new Remote Insight Lights-Out Edition II offers enhanced graphical remote console performance and advanced virtual administration for ultimate control of ProLiant servers.

What's New (Firmware 1.10 *or* Later)

Directory Services Integration
Linux Client Browser Support

Auxiliary Power

On ProLiant servers with the Remote Insight 16-pin or 30-pin connector, the Remote Insight Lights-Out Edition II can obtain its power from the auxiliary power plane of the server by using the internal 16 or 30 pin cable. If the server provides Redundant Power Supplies (RPS) then Remote Insight Lights-Out Edition II will use redundant power and will continue operation in the event of a power supply failure. The external power adapter is not required when using the internal 16-pin or 30-pin cable.

Remote Insight Lights-Out Edition II Kit Contents (PN 227251-001)

Remote Insight Lights-Out Edition II
External Power Adapter
Power Cord(s)
Keyboard-Mouse Adapter Cable
HP Management CD
SmartStart and Support Software CD
Documentation CD
Virtual Power Button Cables (16 pin, 30 pin, 4 pin)

(**NOTE**: When using the 16-pin or 30-pin cable, the Keyboard-Mouse Adapter Cable and External Power Adapter are not required. The 16-pin & 30-pin cables provide keyboard-mouse signal pass through to Remote Insight Lights-Out Edition II remote console. These cables also provide auxiliary power to the Remote Insight Lights-Out Edition II, eliminating the need for using the external power adapter. Some exceptions apply. Refer to the slot and cable matrix available at http://www.hp.com/servers/ lights-out for Remote Insight Lights-Out Edition II cable requirements on ProLiant servers.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 802
Doc. 3608

E C T
1 8407 A
L - A C I

Product Highlights

Security

Using industry standard Secure Sockets Layer (SSL), all HTTP data is encrypted across the network, ensuring the highest level of protection. Configurable access rights for users and encrypted passwords provide protection from unauthorized access. Numerous additional security features include 128-bit encryption of remote console session, event generation for failed login attempts, enforced delay after unsuccessful login attempts, configurable IP port assignments, optional inbound IP address verification/lockout for each user, and optional lockout for the remote console telnet port.

External Power Backup

An external power adapter provides continuous power backup to the board allowing continuous access to the server, even when there is a server power failure or the server has been turned-off.

Reset and Failure Sequence Replay

Remote Insight Lights-Out Edition II captures and replays server video text to assist in locating startup problems and causes of failure.

Insight Manager and Web-Enabled Agent Integration

Remote Insight Lights-Out Edition II fully integrates with Insight Manager 7 under key operating environments providing full SNMP management. It also provides seamless access to the host server's web-enabled agents. Insight Manager also allows detailed diagnostics of the card, ensuring that the card is always online.

Easy to setup and use

An onboard ROM-based configuration utility allows fast and easy setup without additional software. The Remote Insight Lights-Out Edition II can also be setup via the browser interface over the network. Integration with SmartStart Scripting Toolkit allows configuration of the card as part of the initial server deployment. For large deployments of Remote Insight Lights-Out Edition II cards, the HP Lights-Out Configuration Utility can be used to configure in a group fashion, saving time and resources.

Group Administration & Action

Group administration simplifies an IT administrator's task of configuring and managing largely deployed Remote Insight Lights-Out Edition II cards. Using the HP Lights-Out Configuration Utility, an administrator can easily configure network and global settings for a group of cards, rather than one at a time. This can be performed in a batch process or by using Insight Manager 7's powerful device query mechanism. Remote Insight Lights-Out Edition II also allows group actions on one or many servers including power on/off, power cycle, ROM upgrades, and even remote deployment of servers.

Alert Administration

It provides support for SNMP trap delivery to a Insight Manager 7 or any other management console. Traps forwarded by the board can be configured in Insight Manager for delivery to an administrator's pager or e-mail.

Integrated Management Log

It maintains a copy of the host server Integrated Management Log, that can be accessed using a standard browser even when the server is not operational.

Remote Insight Event Log

It includes a detailed event log independent of operating system, which records user actions like server power on/off, reset, changes in user configuration, clear event log, successful and unsuccessful login attempts, enabling auditing of user actions by the supervisor.

Survey

Using a supported browser you can view the HP survey configuration file, which provides the latest host server configuration information to assist in the diagnostic process. Survey is supported on Windows NT®, Windows 2000, Windows Server 2003, and NetWare.

Microsoft EMS Console

The Microsoft Emergency Management Service console provides a text-based screen to access the host server. The Emergency Management Service console option will be available on HP ProLiant servers using Windows Server 2003.

Headless Server Deployment

Enables deployment of headless servers in a data center, eliminating the need to have a monitor, keyboard, mouse, and switch box in every rack. Provides superior cable management with by reducing the required cables from five to three per server.

Technical Specifications

Architecture	32-bit PCI-based remote management board (32-bit slot on primary bus)
Processor	PowerPC 405 GP 200 MHz embedded processor
Upgradability	Option firmware upgradable via flash ROM.
Video Support	Onboard VGA, 640 x 480 (256 to 16.7 M colors), 800 x 600 (256 to 16.7 M colors), 1024 x 768 (256 to 65 K colors), 1280 x 1024 (256 colors)
Interfaces	External power connector One keyboard/mouse input/output One video output One Ethernet network connection (10/100 Mb/s)
External Power Adapter	9 V DC, 1 A
Memory	4-MB flash ROM 32-MB RAM 8-MB video RAM
Remote Insight Server Operating System Support	Microsoft Windows NT 4.0 Server, Terminal Server Microsoft Windows 2000, Advanced Server, Data Center, Terminal Server Microsoft Windows Server 2003, Standard Edition and Enterprise Edition Novell NetWare 5.1, 6.0 Red Hat Advanced Server 2.1, Red Hat Linux 7.3, 8.0 SuSE Linux Enterprise Server V7, V8
Remote Insight Client Operating System Support	Windows 2000 Professional, Windows XP Pro, Windows 2003, Red Hat Advanced Server 2.1, Red Hat Linux V7.3, V8.0 SuSE Linux Enterprise Server V7, V8
Directory Services Support	Active Directory V1.0 (Windows 2000, 2003) Novell eDirectory V8.6.2, V8.7 (Novell NetWare 5.X, 6.X, Red Hat 7.1, Windows 2000, Windows 2003)
Remote Insight Client Browser Support	Internet Explorer 5.5 SP1, 6.0 Netscape Navigator 6.2 (on supported Windows and Linux client systems) Mozilla 1.0 (for supported Linux client systems)

COMPATIBILITY

Servers

For an updated list of supported servers, visit http://h18013.www1.hp.com/products/servers/management/riloe2/supported-servers.html

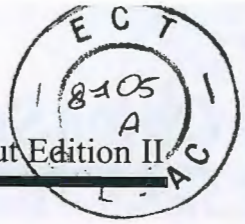
NOTE: The Remote Insight Lights-Out Edition II USB Virtual Media feature is not supported on the 2.40 and 2.80 GHz versions of the ProLiant DL380 G3 and ProLiant ML370 G3 servers. The Remote Insight Lights-Out Edition II cannot be used to connect the local client floppy and CD devices as USB virtual devices to the remote server. All other Remote Insight Lights-Out Edition II features are supported on these servers. The non-USB based Remote Insight Lights-Out Edition II Virtual Floppy feature is still supported, allowing you to perform functions such as remote ROM upgrades and server deployment. The Virtual Floppy feature requires loading the floppy image in to the Remote Insight Lights-Out Edition II. For more details, please refer to the user guide of the Remote Insight Lights-Out Edition II.

© Copyright 2003 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice.

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 803
Doc. 3606



Related Options

Related Options	Virtual Power Button Cable, Remote Insight Board, for HP NetServers **NOTE**: Not required for ProLiant servers.	306121-B21

NOTE: Supported on the following HP Netservers: LC 2000, LH3000/3000r, Tower Server tc3100, Tower server tc4100. Please see the following Web site for the HP ROM Configuration Utility for Netservers: http://www.hp.com/servers/lights-out

Virtual Power Button Cable Kit Contents (PN 306121-B21)

Supported Server	Part Number
tc4100	303291-001
tc3100	303292-001
lc2000	303293-001
lh3000	303294-001

Power Cord Option Kit

These cables are designed for connecting RILOE cards to high voltage PDUs. Each cable can connect up to two RILOE cards.

Remote Insight Board High Voltage Power Cord	201493-001 (single cable)
Remote Insight Board High Voltage Power Cord Multi	201493-002 (pack of 20)

Warranty

One-year, limited warranty – Certain restrictions and exclusions apply. Consult the HP Customer Support Center at 1-800-652-6672 for details.

Apêndice IJ

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 801
Doc.

AVAILABLE PACKS AND PURCHASE INFORMATION

Models

***ProLiant*™ Essentials Integrated Lights-Out Advanced Pack** (Featuring: sophisticated virtual administration features for ultimate control of servers in the data centers and remote sites)
263825-B21 (Software Option Kit – 1 Server)
302280-B21 (Flexible Quantity License Kit)
302281-B21 (License-Only – for use with a Master License Agreement)

Licensing and Packaging

One license is required for every server on which the product is installed and used. Licenses are non-transferable. Full details are contained in the End User License Agreement.

Software Option Kit – 1 Server

Contains one license with a unique license activation key and product documentation. For use with a single server.

Flexible Quantity License Kit

The quantity ordered of this part number will be the quantity of licenses included in the kit along with a corresponding activation key. Use the same key to activate all licenses up to the actual quantity ordered. For a given order, one kit will be delivered with the licenses, activation key, and a single set of product documentation.

License-Only

For use with signed and implemented Master License Agreements only. Purchase of this part number entitles you to deploy another license of the product under the terms of your Master License Agreement. Note: nothing is delivered in conjunction with the purchase of this part number. Visit http://www.compaq.com/proliantessentials for more information on Master License Agreements.

To order the ProLiant Essentials Integrated Lights-Out Advanced Pack contact your Compaq Account Manager or Compaq Authorized Reseller, or go online at http://www.compaq.com/manage/remote-lightsout.html

For more information regarding ProLiant Essentials Software and the ProLiant Essentials Integrated Lights-Out Advanced Pack visit http://www.compaq.com/manage/remote-lightsout.html

For additional information on other Compaq Intelligent Manageability products and services, visit http://www.compaq.com/manage

OVERVIEW

The ProLiant Essentials Integrated Lights-Out Advanced Pack provides Compaq ProLiant Customers with an easy upgrade to full Lights-Out functionality on their Integrated Lights-Out Standard enabled ProLiant servers. The Integrated Lights-Out Advanced Pack features Virtual Graphical Console and Virtual Floppy Drive that offer IT managers with true virtual presence and control to their distributed remote sites and data centers. Using the Integrated Lights-Out Advanced, IT managers can perform all the "in-front-of-the-server" functions such as deployment, diagnostics, ROM upgrades, configuration, and maintenance without physically visiting the server. All this functionality is accessible through a standard browser without requiring special software or use of valuable PCI slot. The Integrated Lights-Out Advanced improves the efficiency of the IT managers who have too many servers to manage, are short-staffed and working with limited budgets. Integrated Lights-Out Advanced results in significant cost savings from reduction of travel costs or requirement of dedicated IT staff for managing servers at distributed sites. Integrated Lights-Out offers added advantage in the dense data centers where space floor is at a premium. Integrated Lights-Out Advanced enables deployment of servers in a "headless" fashion in data center racks by eliminating the need for monitor, switch box, keyboard, mouse, and extra cabling associated with them. The ProLiant BL p-class blade systems ship from the factory with the Integrated Lights-Out Advanced features enabled, allowing the administrators to have full use of the robust Graphical Remote Console and Virtual Media capabilities.

COMPAQ

RQS nº 03/2005 - CN
CPMI - CORREIOS
805
Fls. Nº
Doc.

PROLIANT ESSENTIALS INTEGRATED LIGHTS-OUT ADVANCED PACK BENEFITS

- **Benefit 1** – Integrated Lights-Out Advanced can be easily activated online with a license key requiring no additional software installation or firmware upgrade. Using the Compaq Lights-Out Configuration Utility, the license key activation can be scripted for a group of Integrated Lights-Out processors.
- **Benefit 2** – The ability to view the server console seamlessly and controlling the virtual media devices remotely, frees up the IT staff to organize its personnel more effectively, reduce costs of onsite staff or traveling administrators, and resolve problems more quickly.
- **Benefit 3** – Integrated Lights-Out Advanced supports increased server density in data centers by displacing the need to have monitor, switch box, keyboard, mouse, and associated cables in every rack, resulting in additional cost savings.

PRODUCT FEATURES

Virtual Graphical Console

Integrated Lights-Out Advanced provides embedded hardware Graphical Remote Console capabilities that can turn a supported browser into a virtual desktop, giving the user full control over the display, keyboard, and mouse of the host server. The operating system-independent console supports graphic modes that display remote host server activities, such as shutdown and startup operations. It works with a standard browser and no additional software is required on the remote server or client system.

Virtual Floppy Drive

With the Virtual Floppy Drive, an administrator can easily direct a remote host server to boot and use standard media from anywhere on the network, thus saving time and increasing efficiency by eliminating the need to visit a remote server to insert and use a diskette. Administrators can apply *ROMPaq*™ upgrades to remote servers, deploy an operating system on remote servers from network drives or by using the *SmartStart*™ Scripting Toolkit, or perform disaster recovery of failed operating systems. For operating systems that support Universal Serial Bus (USB) floppy drive devices, the Integrated Lights-Out Virtual Floppy is available "end-to-end", from Boot Time, through OS loading and while the OS is operational.

COMPLEMENTARY PRODUCTS

ProLiant Essentials Foundation Pack* (shipped with every Compaq ProLiant Server)

ProLiant Essentials Workload Management Pack

Compaq Remote Insight Board Lights-Out Edition

Compaq *Insight Manager*™ 7

ProLiant Essentials Rapid Deployment Pack

Compaq SmartStart Scripting Toolkit

** May be named the Server Setup & Management Pack in some servers*

SPECIFICATIONS

Upgradability	Option firmware upgradable via flash ROM
Client Browser Support	Microsoft® Internet Explorer 5.5 or later
Supported Operating Systems	Microsoft Windows® NT® 4.0 Server and Enterprise Edition Windows 2000 Server and Advanced Server Windows .NET Server and Advanced Server Red Hat® 7.2 Professional, Red Hat 7.3 Professional, Red Hat 7.2 Advanced Server SuSE® Linux® Enterprise Server 7 Novell® NetWare® 5.x, 6.x
Client System Support	Microsoft Windows 98 Windows 2000 and 2000 Professional Windows 2000 XP Professional Edition
Supported Servers	Please see the following URL for the latest list of supported servers: http://www.compaq.com/manage/supported-servers.html
Driver Support	Compaq Health Driver (Compaq iLO Advanced Server Management Controller Driver) Compaq iLO Management Interface Driver
Other Product Information	For more information on Integrated Lights-Out, please visit http://www.compaq.com/manage/remote-lightsout.html
Warranty	• Compaq will replace defective delivery media replacement for a period of one year (12 months) following the date of purchase • Startup technical software support - Available for no additional charge by calling Compaq Support up to 90 days from the date of purchase. This includes phone support to assist customers with installation, set-up and product usage questions and/or problems. Worldwide numbers for Compaq Support are available at: http://www.compaq.com/support/contact_compaq/index.html. .

© 2002 Compaq Information Technologies Group, LP.
Compaq, the Compaq logo, Insight Manager, Proliant, ROMPaq, and SmartStart are trademarks of Compaq Information Technologies Group, L.P. in the U.S. and/or other countries. Microsoft and Windows NT are registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries. Red Hat is a registered trademark or trademark of Red Hat, Inc. in the US and other countries. Linux is a registered trademark or trademark of Linus Torvalds in the U.S. and/or other countries. SuSE and its logo are registered trademarks or trademarks of SuSE AG in the U.S. and/or other countries. NetWare and Novell are registered trademarks or trademarks of Novell Inc., in the U.S. and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 806
3608
Doc.

Apêndice IL

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3693
Doc.

1 8610 A- CPL - AC

capacity	Superdome provides a computing utility infrastructure unmatched by any competitor. Superdome's superior system and processor architecture provides scalability that outstrips the competition.
connectivity	Superdome offers massive amounts of I/O connectivity. And it has high-speed connectivity, too.
security	Thanks to HP Virtualvault and other leading security products, Superdome can offer unparalleled levels of security. Virtualvault today has been entrusted to protect some $7 trillion in assets, testimony to its industry-wide acceptance.
manageability	HP's suite of management products are all ready to make Superdome management easier. And with its dynamic new capabilities as part of the HP Partitioning Continuum, Superdome provides the best combination of system flexibility and convenient management.
for more information	Looking for more information about HP's Superdome? • For more information about performance and scalability, please refer to the Superdome Performance White Paper. • For more information about high availability, please refer to the Superdome High Availability White Paper. • For more information on Superdome services, go to: www.hp.com/go/superdome

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 808
Doc. 3698

For more information, contact any of our worldwide sales offices or HP Channel:

For the location of the nearest sales office call:
United States of America: +1 800 637 7740
Canada:
Hewlett-Packard Ltd.
5150 Spectrum Way
Mississauga, Ontario L4W 5G1
+1 905 206 4725
Japan:
Hewlett-Packard Japan, Ltd.
Japan Country H.Q.
3-29-21, Takaido-Higashi, Suginami-ku,
Tokyo, 160-8585 Japan
+81 3 3331 6111
Latin America:
Hewlett-Packard
Latin American Region Headquarters
Waterford Building, 9th Floor
5200 Blue Lagoon Drive
Miami, Florida 33126 USA
+1 305 267 4220
Refer to country phone numbers
Australia/New Zealand:
Hewlett-Packard Australia Ltd.
31-41 Joseph Street
Blackburn, Victoria 3130
Australia (A.C.N. 004 394 763)
+61 3 9272 2895
Asia Pacific:
Hewlett-Packard Asia Pacific Ltd.
17-21/F, Shell Tower
Times Square
1 Matheson Street
Causeway Bay
Hong Kong
+8522 599 7777
Europe/Africa/Middle East:
Hewlett-Packard S.A.
150, Route du Nant-d'Avril
CH-1217 Meyrin 2
Geneva, Switzerland
+41 22 780 81 11
European Multicountry: +41 22 780 81 11
Middle East and Africa: +41 22 780 71 11
European Headquarters: +41 22 780 81 81
Refer to country phone numbers

For direct country contact call:

Argentina: +541 787 7145

Austria: +43 1 25 000 0

Belgium and Luxembourg: +32 2 778 31 11

Brazil: +5511 7296 8000

Chile: +562 203 3233

Colombia: +571 629 5030

Denmark: +45 45 99 10 00

East Central Europe, CIS, and Yugoslavia:
+43 1 25 000 0

Finland: +358 9 887 21

France: +33 1 69 82 60 60

Germany: +49 7031 140

Greece: +30 1 689 644

Hungary: +36 1 252 7300

Iceland: High Performance Systems hf.
+354 1 67 10 00

Ireland: +353 1 615 8200

Israel: Computation and Measurement Systems
(CMS) Ltd. +972 3 5380 333

Italy: +39 2 92122770

Mexico: +525 326 4600

Netherlands: +31 20 547 6911

Norway: +47 22 7356 00

Poland: +48 22 608 77 00

Portugal: +351 1301 7343

Russia and the CIS, excl. Ukraine:
+7 095 923 5001

Slovenia: +38 61 55 84 72

Spain: +34 1 631 1600

Sweden: +46 8 444 2000

Switzerland: +411 735 7111

South Africa: Hewlett-Packard South Africa
(Pty) Ltd.+27 11 806 1000

Turkey: +90 212 224 5925

United Kingdom: +44 1344 369231
Venezuela: +582 239 4133

Full information on HP products is available at **www.hp.com**

Intel and Itanium are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries and are used under license. Java is a U.S. trademark of Sun Microsystems, Inc. UNIX is a registered trademark of The Open Group. Windows and Windows NT are U.S. registered trademarks of Microsoft Corporation.

The information contained in this document is subject to change without notice.

© Copyright Hewlett-Packard Company 2001.

05/02

5980-7679EN Rev. 1

invent

ECT 8672 A. CPMI - AC

superdome and hp-ux 11i

HP-UX 11 is HP's complete 64-bit UNIX operating environment that delivers significant scalability and performance for demanding applications. And the latest version of HP-UX is HP-UX 11i. When teamed with HP's leading server systems, HP-UX 11i provides the power of supercomputing at a fraction of the cost.

features of hp-ux 11i

HP-UX 11i offers:

- Excellent compatibility with Windows and Linux.
- Comprehensive Internet-critical functionality.
- Ultimate performance and scalability, including 64-way SMP support for Superdome.
- Industry-leading investment protection through binary compatibility.
- Superdome management features, including partition management.
- Support for nPartitions and virtual partitions.
- Excellent high availability features such as online addition and replacement for I/O and networking cards, dynamic patching, dynamically tunable kernel parameters, and up to 70 percent faster rebooting.
- Middleware and application software forward compatibility from HP-UX 11.0.

HP-UX 11i delivers an end-to-end scalable, manageable, and secure infrastructure for developing, deploying, and brokering mission-critical e-services. It has features targeted at Internet applications, and it contains functionality for managing Superdome servers.

hp-ux 11i operating environments

With HP-UX 11i, ordering and configuration have been vastly simplified. HP-UX 11i is available in three operating environments, as shown in **figure 9**. Each consists of basic HP-UX plus a collection of layered software products addressing your specific needs for availability, manageability, and security. These environments are simple to install and maintain, and they are a great value to purchase.

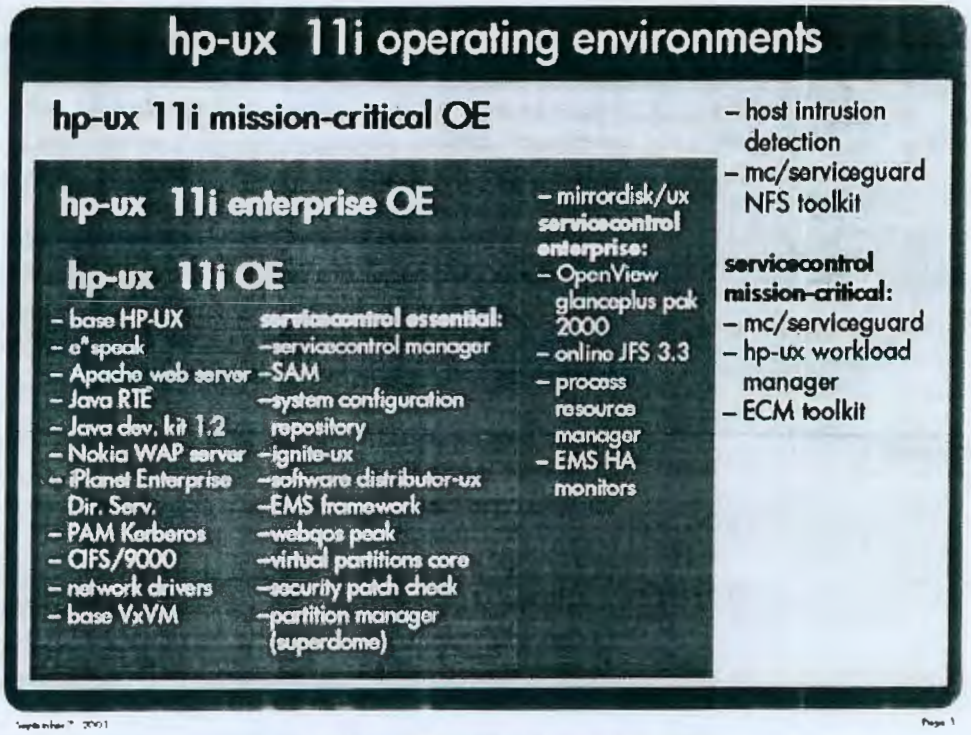


figure 9: hp-ux 11i operating environments

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 809
Doc. 3698

entry-level hp-ux 11i

The entry-level operating environment offered with every server addresses key needs from a Web and small application perspective. And new Superdome-specific functionality, such as Partition Manager, is tightly integrated with the base HP-UX. The core functionality of the new virtual partition capability is also included.

hp-ux 11i enterprise

The HP-UX 11i Enterprise OE is targeted at larger application servers typically served by mid-range systems such as the HP Server rp7410. Customers in this environment usually need
to optimize resources and do proactive capacity planning with higher uptime; so the Enterprise OE includes tools such as Process Resource Manager, Glanceplus Pak, and Mirrordisk/UX.

hp-ux 11i mission-critical

The mission-critical OE is highly recommended for most Superdome systems because it specifically addresses the needs of large application and database server environments. This operating environment includes host intrusion detection to protect the system from outside attackers, MC/Serviceguard for the highest degree of HA, and HP-UX Workload Manager for automatic resource allocation based on set service levels. Goal-based resource allocation is a must in today's Internet world, and HP is today the *only* UNIX vendor offering such sophisticated resource allocation capability.

the rest of the superdome story

This white paper has barely touched the surface of Superdome's capabilities. Here are some other areas of interest.

the always-on infrastructure and superdome

Because no Superdome stands in isolation, you can expect even more from HP. Superdome can be part of your always-on infrastructure, meeting the needs of your total IT environment throughout the life of the solution.

Superdome is delivered with a Foundation Configuration of services that ensure you get the right configuration for your solution the first time, and in record time. The services begin with up-front assessments of business/IT alignment, IT technical skills, and environment and mission-critical readiness. You'll also get a detailed architecture design based on your solution; factory pre-integration for software, peripherals, and middleware; and an HP solution manager assigned to ensure your satisfaction. You'll also be able to add mission-critical support services to meet the demanding requirements for stability and availability so characteristic of the Internet powerhouse.

peripherals and superdome

Superdome peripherals are supported through industry-standard PCI. The PCI FWD SCSI host adapter provides a fast and wide (FWD) SCSI interconnect currently available at 40 MB/s. This adapter provides an ideal interface to high-performance disk array subsystems and high-performance tape drives.

mass storage and superdome

Superdome supports a wide range of mass storage options, including several varieties of SCSI-attached RAID, Fibre Channel-attached RAID, SCSI-attached tape drives and tape libraries, and Fibre Channel-to-SCSI multiplexer connections.

conclusion

In this era of 24 x 7 applications and mission-critical Internet operations, businesses need a bulletproof infrastructure. That infrastructure is powered by HP's industry-leading, high-performing, enterprise servers and the robust HP-UX 11i operating environment. And Superdome represents another giant step forward for the HP server line.

availability

With its industry-leading multi-system availability, single-system reliability, and superior nPartition resilience, Superdome is designed to meet the needs of large enterprises, service providers, and established online economy companies.

increased flexibility via support of multiple environments

Business requirements and competitive pressures can dictate the need for a large set of applications, both old and new. Often applications require different versions or revisions of operating systems, different system parameter settings, and even different patch levels. Performance can suffer from the interactions of applications with incompatible behaviors.

Superdome nPartitions can provide multiple independent environments for these applications. For instance, with nPartitions a portion of the compute and I/O resources can be configured to run an old copy of the operating system, while the rest of the machine is updated to run the newer software. Or you can use nPartitions to set up a test environment where new software and operating systems can be installed while leaving production applications to continue operation without impact.

Future releases will provide the ability to run different operating systems such as HP-UX, Linux, and Windows on the same Superdome platform. And for an even higher degree of flexibility you can run virtual and resource partitions within an nPartition—and change them on the fly—to even further optimize your resource utilization.

increased uptime

nPartitions provide independence of failure or operation. If you have to reboot one nPartition or take it down to perform an operating system upgrade, the other nPartitions in the system are not affected.

Unlike a traditional large SMP, nPartitions allow a server to be configured into a cluster of independent systems. Since failure independence is provided by nPartitions, high availability clusters, consisting of two or more nPartitions, can be configured within the same server to improve single-system availability. In addition, you can configure MC/Serviceguard to fail over applications from one nPartition to another nPartition within the same Superdome system or to another HP Server.

increased scalability

Some applications may not have the ability to scale linearly with large numbers of CPUs. Superdome's nPartitions allow you to tailor the processor, memory, and I/O resources to match application scaling characteristics. What's more, as new application or operating system releases provide improved scaling characteristics, nPartitions allow the resources to be readjusted to optimize application performance.

superdome: ease of management

In spite of all its power and flexibility, the Superdome system is remarkably easy to manage, making your life easier with a host of management features and technologies. These include:

- Superdome Support Management Station
- Partition Manager
- Servicecontrol suite

superdome support management station

The Support Management Station (SMS) is used to run Superdome scan tools. These are the same scan tools used to enhance diagnosis and testability of the platform throughout Superdome development and manufacturing, and they are now available to HP field engineering organizations. This translates into better management, as well as faster and easier upgrades and hardware replacement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 810
Doc. 3698

SMS installation

One SMS is installed per customer site (or data center), connected to each Superdome platform via a private LAN. (Ideally, the SMS is installed near the associated Superdomes, because the HP Customer Engineer will run the scan tools and then be able to immediately make any necessary hardware repairs.) The physical connection from the platform is a private Ethernet connection.

The SMS can support two LAN interfaces:

- The dedicated connection to the systems to be supported.
- The connection to interface with the customer's general LAN.

These two LAN connections allow SMS operations to be performed remotely. More than one SMS can exist on a private LAN, but only one SMS should be actively using the LAN.

SMS functional capabilities

Here's what the SMS can do:

- Allows remote access via customer LAN (no modem access).
- Can be disconnected from the Superdome platform(s) and not disrupt their operation.
- Can connect a new Superdome platform to the SMS and be recognized by scan software.
- Supports multiple, heterogeneous Superdome platforms with scan software capability.
- Can scan one Superdome platform while other Superdome platforms are connected, without disrupting the operational platforms.
- Can run the scan software tools.
- Can run up to four scan processes concurrently, each on a different Superdome platform.
- Supports utility firmware updates.

partition manager

Another invaluable management feature for Superdome is Partition Manager. This tool provides control and management of Superdome nPartitions. You can launch it as a GUI from system administration manager (SAM) or directly from the command line, and with it you can:

- Display server status.
- Create and modify nPartitions.
- Display a complete hardware inventory.
- Display status of key server components.
- Check for problem or unusual server conditions.
- Manage power to cells and I/O chassis.
- Toggle attention indicators for cells, I/O chassis, I/O cards, and cabinets.

se ecntrol suite

HP's Servicecontrol suite addresses the requirements for centralized configuration, fault, and workload management, providing effective, efficient management of computing resources.

- HP Servicecontrol provides cost-effective control through truly multi-system management tools allowing rapid deployment, consistency, and asset management.
- Fault management in the Servicecontrol suite adds the full power of monitoring and proactive problem solving.
- Servicecontrol suite's workload management tools enable administrators to optimize Web and application workloads via dynamic resource allocation.

The different components of the Servicecontrol suite are tightly integrated into all the HP-UX 11i operating environments.

8676
A.

virtual partitions

Virtual partitions provide even more portioning granularity, and HP's virtual partitions are unique in the UNIX industry. Superdome supports up to 16 nPartitions and up to 64 virtual partitions. So a system with 16 nPartitions can have as many as four virtual partitions in each nPartition—or, to put it another way, one virtual partition per CPU. Each virtual partition runs its own image of the HP-UX 11i operating system and can fully host its own applications.

This solution offers complete software isolation across virtual partitions. Software isolation guarantees that an application running in one virtual partition is not affected by a software crash in another. Although virtual partitions are susceptible to hardware failures, protection against hardware failures is provided with Hyperplex or nPartitions. Virtual partitions also let you dynamically adjust partition size (without rebooting) by the dynamic addition and deletion of CPUs, effectively moving them from one virtual partition to another.

resource partitions

Very often many applications run on one server at the same time, but each application has different resource needs. (As an analogy, think of electricity use: many homes use electricity from the same generator, but some homes need more power than others.) HP's resource partitions are unique partitions created just for this type of workload management.

Resource partitions run within hard partitions or virtual partitions, and are controlled by workload management functions within the operating environment. HP-UX Workload Manager (WLM) and Process Resource Manager (PRM) software dynamically create resource partitions for applications that need guaranteed amounts of dedicated resources such as CPU cycles, memory, or disk I/O. Applications with specific goals, such as response time, can use HP's goal-based HP-UX WLM to automatically and dynamically allocate the necessary resources to applications or user groups within hard partitions or virtual partitions. With resource partitions and workload management tools, varying service level objectives can be met every time!

how nPartitions work

Within Superdome, cell boards are grouped into physical structures. An nPartition consists of one or more cells that communicate coherently over a high-bandwidth, low-latency crossbar fabric. Special programmable hardware in the cell boards defines the boundaries of an nPartition in such a way that isolation from the actions of other nPartitions is enforced.

Each nPartition runs its own independent operating system, and different nPartitions can be executing the same or different versions of an OS. In a Superdome IPF system, they can even be executing different operating systems altogether (such as HP-UX, Linux, and Windows).

Each nPartition has its own independent set of CPUs, memory, and I/O resources. You can use system management commands to change resources from one nPartition to another without having to physically change the hardware. Moreover, using the dynamic reconfiguration capabilities of HP-UX 11i , such as online addition and removal, you can add new resources to an nPartition and delete resources while the nPartition remains in operation. In addition, dynamic additions of new nPartitions are supported.

uses for nPartitions

With nPartitions, you can configure Superdome as one large symmetric multiprocessor or as several independent nPartitions. Using independent nPartitions has advantages in several areas: increased systems utilization, increased flexibility by supporting multiple environments, increased uptime, and increased scalability.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 811
Doc. 3698

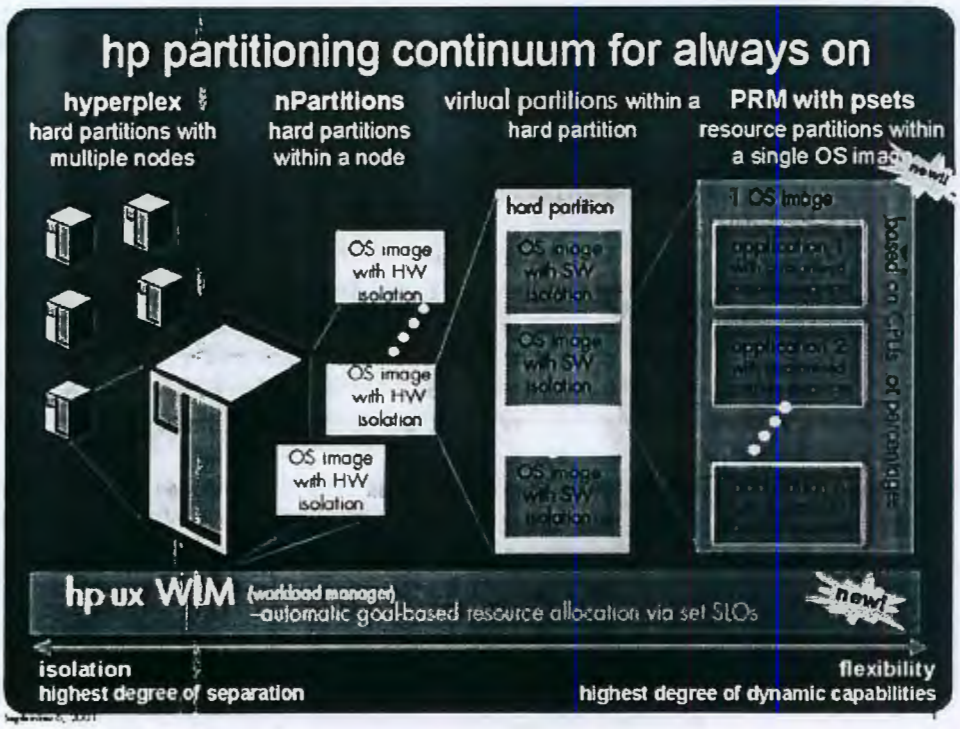


figure 8: using superdome's partitioning continuum

increased systems utilization

Businesses today require that multiple applications running on the same server deliver full performance without conflicting or interfering with one another. It is critical that the actions of one application do not impact other applications or result in denial of service to them. Furthermore, a single failure in the operating system or hardware components on the server supporting the set of applications must not result in the loss of multiple applications running on that server.

Superdome nPartitions are the answer. With Superdome nPartitions, each nPartition is isolated from the others. The dynamically configurable hardware provides an effective firewall between applications so that there is virtually no possibility of interference between nPartitions. The result is increased systems utilization with security—the perfect answer for systems consolidation scenarios.

binary compatibility for across PA-RISC

You can continue to rely on binary compatibility across the PA-RISC family, enabling seamless interoperability with legacy applications on HP systems. Binary compatibility protects your investments, enabling rapid growth and adoption of new technology infrastructures. For performance improvements, you can use existing applications and operating systems with new or more advanced processor technology as it develops.

binary compatibility for Itanium Processor Family

HP will continue to support binary compatibility through the introduction of Itanium Processor Family based systems. As a result of HP's work with Intel® on EPIC (Explicitly Parallel Instruction Computing) architecture, the technology foundation for the Itanium Processor Family, today's HP-UX, Windows 2000, and Linux applications will run unchanged on the Itanium Processor Family. To ensure maximum performance, you can recompile applications without source changes.

upgrading a superdome system

Upgrading an existing Superdome system is as simple as removing all the cell boards and the memory contained on them. You transfer the memory to the new processor cell boards, plug the cell boards into the cabinet, and resume operation.

In the future, Superdome will be upgradable to follow-on PA-RISC processors and to IPF processors. A new cell board and power conversion card are required.

Processor upgrades occur on a cell board basis and can be performed one nPartition at a time in order to minimize downtime for the entire Superdome complex. You can upgrade either PA-RISC or IPF processors in this manner (although mixing PA-RISC and IPF processors in one system is currently not supported).

Today's Superdome is already prepared for the next generation of processors, ensuring that Superdome will stay ahead of tomorrow's performance demands. Whether it's a PA-RISC or an IPF follow-on processor, Superdome delivers the investment protection afforded by in-chassis upgrades.

superdome partitioning

With the addition of Superdome, HP now offers an extremely comprehensive partitioning continuum. Partitions are physical or logical mechanisms for isolating operational environments within single or multiple servers, so that applications can enjoy protection from unrelated events that could otherwise cause disruption, interruption, or performance degradation. Partitioning allows isolating operational environments to ensure privacy and uptime while maintaining the highest degree of flexibility.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 812
Doc. 3698

the hp partitioning continuum

The HP Partitioning Continuum provides a broad range of partitioning solutions designed to meet the diverse needs of our customers. **Figure 7** illustrates the various types of partitions. This is the only UNIX solution on the market to simultaneously address the often contradictory needs of flexibility and uptime.

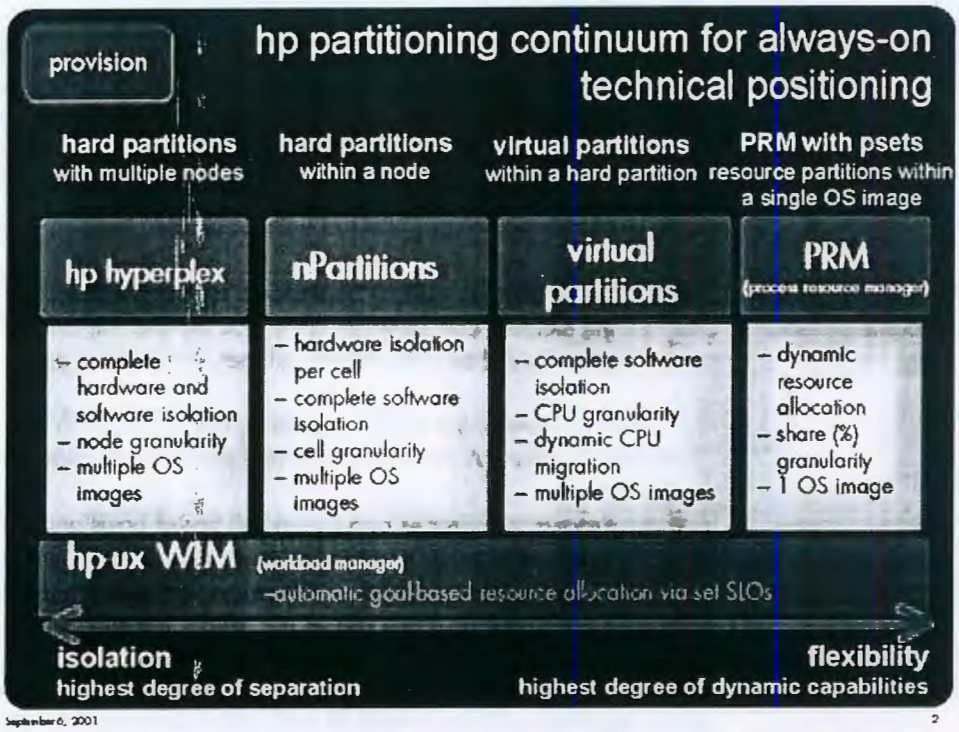


figure 7: hp's partitioning continuum combines high isolation with excellent flexibility

hyperplex: hard partitions with multiple nodes

Hard partitions with multiple server nodes are called the Hyperplex solution. Hyperplex delivers the optimum capacity at all levels by supporting the complete HP UNIX server product line. And Hyperplex is extremely scalable—in fact, a Hyperplex solution can range in size from as few as two entry-level server nodes up to hundreds of the latest Superdome servers, providing the maximum possible capacity.

The hard partitions with multiple nodes afforded by Hyperplex are designed to allow total isolation from other hard partitions. Multiple applications can run in these partitions, and these applications are completely isolated from other nodes and their respective operating environments.

nPartitions: hard partitions within a node

Hard partitions within a node are called nPartitions. A unique feature of HP Superdome servers, nPartitions form the most powerful HP high-end Hyperplex server nodes. A Superdome server can support anywhere from one to 16 nPartitions, each supporting its own operating system, applications, peripherals, and networks. Currently each nPartition can host HP-UX operating environments. When the Intel IPF versions of Superdome are available, nPartitions will support Linux and Windows environments as well.

n+1 fans, power supplies, backplane DC/DC converters

Superdome servers are equipped with N+1 fans, power supplies, and backplane DC converters, ensuring maximum availability for these components.

dual power sources

Dual power sources in Superdome servers mean the power supply can be protected against becoming a single point of failure.

online addition and replacement (OLAR) of PCI I/O cards and chassis

PCI card and chassis OLAR enables the online addition and replacement of PCI I/O cards and chassis on Superdome systems. The system hardware uses per-slot power control combined with operating system support for the PCI card OLAR feature to allow you to add a new card and replace an existing card without affecting other components or requiring a reboot.

online addition and replacement of cell boards

Superdome and a future HP-UX release after 11i support online addition and replacement of cell boards, allowing repair and maintenance of these critical components without bringing the system down.

online addition of nPartitions

With HP-UX 11i, Superdome lets you add nPartitions without affecting other running nPartitions. Such dynamic reconfiguration is another reason why Superdome provides superior uptime. And Superdome is enabled for dynamic cell board migration, which will be fully supported with the next release of HP-UX 11i.

mc/serviceguard in-a-box

In order to increase the uptime of applications within a Superdome system, you can configure nPartitions in an MC/Serviceguard cluster so that the cluster membership is within the system. Upon detection of a failure within an nPartition, MC/Serviceguard fails over the application to another nPartition within the Superdome system.

superdome: investment protection

The Superdome family provides outstanding customer investment protection and lasting value, thanks in part to a system infrastructure designed to accommodate several generations of processor upgrades. For example, Superdome will be board-upgradable to future PA-RISC and IA-64 processors. And all major system components other than the cell board and power conversion card remain the same for PA-8600 or PA-8700 processors; these processors even use the same memory DIMMs. What's even better is the customer's investment in PA-8600 processors is protected, as PA-8600 and PA-8700 processors can be mixed in the same Superdome (but not in the same partition).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 813
Doc. 3698

microprocessor roadmap

The microprocessor roadmap in **figure 6** illustrates how the processors used in Superdome evolved. It also illustrates HP's commitment to long-term processor and architecture innovation, which ensures that HP will continue to provide the massive resources needed for future computing requirements.

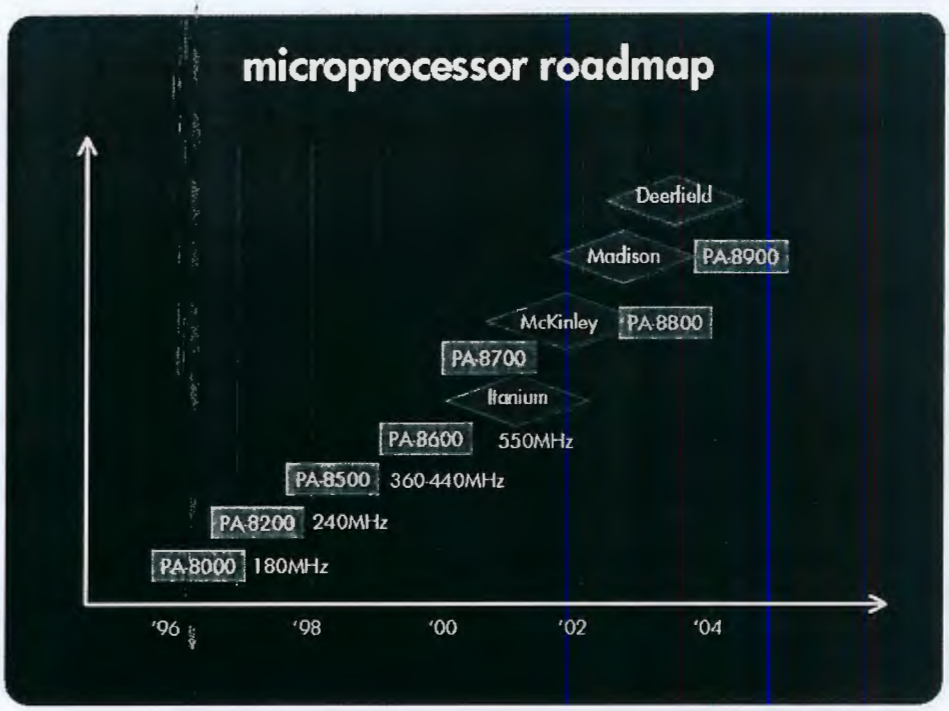


figure 6: hp microprocessor roadmap

The processor roadmap shows not only HP's leading line of RISC processors but also the introduction of binary compatible IPF processors. Notice that HP is investing in several PA-RISC enhancements after the introduction of the IPF; this means you'll be able to move to the new Itanium Processor Family architecture when you're ready, not when forced to by a vendor. Superior microprocessors and binary compatibility help make Superdome the fastest high-end server on the market, and the safest investment for the future.

ECT 18682 A. L. AC

When a hardware monitor detects a problem, it generates an event that can be reported to you via DMI, SNMP, OpenView Vantagepoint Operations, e-mail, page, syslog, console, or a selected text log file. Each event contains a complete description of the problem, a severity classification (informational, warning, serious, critical), and text that shows the probable cause and the action to take.

When excessive processor cache errors are detected, the processor is automatically removed from use until it is replaced.

hardware inventory in support tools manager

With Superdome, HP's Support Tools Manager (STM) has been enhanced to give you detailed information about the system. Superdome has been designed with the ability for each individual field replaceable unit (FRU) to report information such as serial number, part number, revision level, etc. This information is available in the "Miscellaneous" information tool in STM. Moreover, all of the hardware inventory information is accessible via desktop management interface (DMI).

support management station

To decrease the possibility of unscheduled downtime still further, the Superdome Support Management Station (SMS) is a separate server that provides diagnosis and test capabilities for the Superdome system. The SMS includes ASIC-level scan tools that can be used by HP Support Engineers to diagnose Superdome systems in your data center. (For more details of the SMS, see "Superdome Support Management Station" on page 26.)

high availability observatory

Superdome systems can be supported by Hewlett-Packard's High Availability Observatory (HAO), a support solution designed to keep mission-critical environments up and running. The HAO lets HP's Mission Critical Support Centers reduce the number, duration, and impact of outages on covered systems.

The HAO is a state-of-the-art suite of tools, processes, and support personnel that combine to provide significant support capabilities for systems covered by mission-critical HP support contracts. The HAO solution improves the availability of Superdome systems by:

- Conducting frequent, automated data collection of the customer's mission-critical environment
- Providing a secure, high-bandwidth link for HP support personnel to remotely access the customer's environment to conduct diagnostic tests and potentially solve reported problems
- Providing reactive and proactive support for HP's mission-critical customers

In addition to covering Superdome and HP-UX 11i, HAO technology covers HP-UX servers running HP-UX 10.20 and 11.0, as well as HP, Dell, and Compaq servers running Windows NT® 4.0 (with Service Pack 3 or later) or Windows® 2000, as these systems are identified in your mission-critical support contract. Network interconnect devices, such as hubs, switches, bridges, and routers manufactured by HP and Cisco, are also covered by HAO tools.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 811
3698
Doc.

T
681
A
CPL. AC

There are three major architectural components of the HAO: the HP Support Node, the high-bandwidth secure link, and the Mission Critical Support Center (MCSC).

- **HP Support Node:** This is an HP-owned and operated HP workstation that resides within your environment. Its job is to act as the depot for various tools that capture your system configurations and network topologies for use by HP support personnel. HAO tools residing on the HP Support Node collect the configuration information and send it to one of HP's Mission Critical Support Centers. The HP Support Node also serves as an HP-managed resource to analyze core dumps and help with other reactive support. The HP Support Node is the entry point for HP support engineers to access your mission-critical systems.
- **High-Bandwidth Secure Link:** The high-bandwidth secure link, or ISDN link, connects HP and the mission-critical customer. This link provides HP with the capability to react quickly when reactive support requires accessing your systems to help resolve a problem. It also is a path used to transport data from the HP Support Nodes to the MCSC for proactive analysis.
- **Mission Critical Support Center:** The MCSC resides inside HP. Its job is to act as the primary support center to collect and track customer information and to perform proactive problem analysis; it also provides a control point in the HAO remote support architecture. To maintain the security of the your environment, the MCSC allows access to the isolated LAN only to authorized HA (high availability) Support Engineers.

A Remote Support Resource (RSR) is placed inside the isolated LAN, providing a secure method for authorized HA Support Engineers to access customer sites.

Configuration analyzer servers in the MCSC take configuration information collected from all HP Support Nodes and continually analyze the data. If an irregularity is identified, a case is opened in the MCSC's workflow management system. MCSC Monitor, a tool at the MCSC, provides a display of customer enterprise configuration data transported nightly from each HP Support Node. When providing reactive support, HP Support Engineers check the MCSC Monitor for configuration changes, and they can view patch summary information when providing proactive support.

repairability

Superdome servers are endowed with a substantial number of features that make them easier to repair with little or no downtime. Among these features are:

- N+1 CPUs with instant capacity on demand (iCOD)
- Hot-swap N+1 fans, power supplies, and backplane DC/DC converters
- Online replacement of PCI I/O cards
- Online addition/replacement of PCI I/O chassis (follow-on release to HP-UX 11i)
- Online addition/replacement of cell boards (follow-on release to HP-UX 11i)
- Dual power sources

n+1 CPUs with iCOD

With HP-UX 11i, Superdome has support for instant capacity on demand (iCOD). This feature lets you bring additional CPUs online without a system reboot. Because no reboot is needed, the system has no loss of availability, even while you're adding capacity.

Another advantage of iCOD is that it allows setting up a system of N+1 CPUs, ensuring maximum single-system availability. If one CPU fails, another is already running and prepared to take its place.

superdome: performance and scalability

Superdome offers a host of features that are especially important in the OLTP, business intelligence, and technical markets. And bandwidth and scalability are two important areas of Superdome leadership.

system bandwidth

	superdome 16-way	superdome 32-way	superdome 64-way
crossbar bandwidth (peak)	16 GB/s	32 GB/s	64 GB/s
cell controller to I/O subsystem bandwidth (peak)	2.0 GB/s	2.0 GB/s	2.0 GB/s
I/O bandwidth (peak)	8 GB/s	16 GB/s	32 GB/s
memory bandwidth	16 GB/s	32 GB/s	64 GB/s

scalability

	superdome 16-way	superdome 32-way	superdome 64-way	superdome I/O expansion (see note 1)
4-CPU cell boards (hot-swap capability offered with HP-UX releases after 11i)	1–4	1–8	8–16	N/A
CPUs	1–16	1–32	8–64	N/A
memory (with 512-MB DIMMs)	4–64 GB	8–128 GB	16–256 GB	N/A
12-slot I/O card cages	4	4/8	8/16	8
hot-swap PCI I/O slots	48 slots (32 33-MHz slots, 16 66-MHz slots)	48/96 slots (64 33-MHz slots, 32 66-MHz slots)	96/192 slots (128 33-MHz slots, 64 66-MHz slots)	96
nPartitions	4	4/8	8/16	N/A

Note 1: For I/O expansion up to 168 slots, one Expansion Cabinet (6 I/O card cages) is required. For I/O expansion up to 192 slots, two Expansion Cabinets (2 I/O card cages) are required. Any remaining space in the I/O Expansion Cabinets can be used to store peripherals. Both the 1.96m and 1.6m heights are available for the I/O Expansion Cabinet.

For more information about performance and scalability, please refer to the Superdome Performance White Paper.

perdome: high availability

Superdome offers unprecedented single-system availability in the following areas:

- System reliability
- Supportability
- Repairability
- MC/Serviceguard-in-a-Box

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 815
Nº 3698
Doc.

C T —
8683 A C
C P L

superdome: system reliability,

The Superdome product family is bolstered by design enhancements and production techniques that substantially enhance system reliability. Among these enhancements are:

- Memory DRAM fault tolerance—that is, recovery of a single SDRAM failure
- DIMM address parity protection
- Dynamic memory resilience—page de-allocation of bad memory pages during operation
- Dynamic processor resilience
- CPU cache ECC protection and automatic de-allocation
- CPU bus parity protection
- Full single-bit error detection and correction on crossbar and I/O links
- I/O error recovery and system resilience to I/O card failures
- I/O cards fully isolated from each other
- Prevention of silent corruption of data going to I/O
- Recovery of a single I/O-to-cell controller link failure
- Recovery of a single crossbar wire failure
- Localization of crossbar failures to the partitions using the link
- Automatic de-allocation of bad crossbar link upon boot
- ASIC full burn-in and "high quality" production process, resulting in 10X improvement in ASIC failure rates
- Full "test to failure" and accelerated life testing on all critical Superdome assemblies
- Strong emphasis on quality for multiple-nPartition single points of failure (SPOFs)
- System resilience to Guardian Service Processor (GSP)
- Isolation of nPartition failures; failure of one nPartition will not bring down another partition
- Protection of nPartitions against spurious interrupts or memory corruption

supportability

Supportability is another key feature of the Superdome product line. Some of the supportability features of Superdome include:

- Event Monitoring Service (EMS)
- Improved Support Tools Manager
- Support Management Station
- High Availability Observatory (HAO)

event monitoring service

For Superdome, HP's Event Monitoring Service aids in system management by keeping track of the system's "vital signs." EMS lets you monitor virtually all of the hardware on the system, including:

- Mass storage
- Memory
- Fibre Channel components (MUX, switch, card, fabric, etc.)
- I/O cards
- ECC errors on the main system bus
- ECC errors in the CPU cache
- System temperature
- Support processor problems
- Processor dependent hardware problems
- Processor dependent hardware battery low
- Cabinet fans
- Cabinet power supplies
- Chassis code logging failure
- Processor dependent code (firmware) problems

The system hardware configuration and selected kernel parameters are also monitored.

8686

The total crossbar bandwidth for each Superdome model is calculated like this:

(Number of cells x peak crossbar bandwidth per cell) + 2 ports

Crossbar bandwidth for the different Superdome systems is excellent:

- For Superdome 16-way, the crossbar bandwidth is 16 GB/s
- For Superdome 32-way, the crossbar bandwidth is 32 GB/s
- For Superdome 64-way, the crossbar bandwidth is 64 GB/s

memory and backplane latencies

Superdome has been designed to reduce memory and backplane latencies, providing optimum performance. There are three types of memory latencies within the Superdome system:

- *Memory latency within the cell* refers to the case where an application runs on an nPartition that consists of a single cell board.
- *Memory latency between cells on the same crossbar* refers to the case where the nPartition consists of two cells that reside on the same crossbar. In this case, 50 percent of the addresses are to the memory of the requesting processor's cell board and the other 50 percent of the addresses are to the memory of the other cell board.
- *Memory latency between cells on different crossbars* refers to the case where the nPartition consists of cell boards that do not reside on the same crossbar. In this case, if there are 16 cells in the nPartition, 1/16 of the requests are to the memory of the cell board in which the processor resides. 3/16 of the requests go to the memory of the other three cell boards on this same crossbar. Finally, the remaining 12/16 of the requests transit two crossbars.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 816
Doc. 3698

8685 A CPL AC

Superdome memory latency depends on the number of CPUs and the location of their corresponding cell board. Assuming that there is equally distributed access to all memory controllers and that cell boards are installed to minimize latency, the average memory idle latency (when nothing is executing on the system) and memory latency (load-to-use) are shown below.

number of CPUs	average idle latency	average memory latency
4-CPU	174 ns	235 ns
8-CPU	208 ns	266 ns
16-CPU	228 ns	296 ns
32-CPU	261 ns	336 ns
64-CPU	275 ns	360 ns

the I/O subsystem

Superdome cells have remote I/O; this enhances modularity and means there are no trade-offs for scaling of processors, memory, and I/O. Each cell can connect to a remote I/O chassis through an I/O cable link.

Superdome's I/O subsystem has plenty of capability for today and expansion for tomorrow. Each I/O module consists of twelve PCI connections, divided among eight 2X and four 4X PCI slots, with an I/O controller ASIC and power. Each PCI slot has its own PCI bus; the 2X PCI slot has 266-MB/s bandwidth and the 4X PCI slot achieves a bandwidth of 533 MB/s. The point-to-point connectivity allows the earliest detection, containment, and recovery from errors.

Any I/O module can support a core I/O card (required for each independent nPartition). Superdome 16-way, 32-way, and 64-way systems can accommodate four, four, and eight I/O modules, respectively, within the system cabinet. This provides a total of 48, 48, and 96 PCI slots, respectively.

An I/O Expansion Cabinet can also be added. On the Superdome 32-way system, this yields an additional 48 PCI slots, giving a maximum connectivity of 96 PCI slots for 8 cells. For a Superdome 64-way system, the I/O Expansion Cabinet provides an additional 96 PCI slots, for a maximum connectivity of 192 PCI slots for 16 cells.

A system configured with 16 cells, each with its own I/O module and core I/O card can support up to 16 independent nPartitions. Note that cells can be configured without I/O modules attached, but I/O modules cannot be configured in the system unless they are attached to a cell.

The I/O subsystem bandwidth is 2.0 GB/s per cell. This makes the total I/O subsystem bandwidth 8.0 GB/s, 16.0 GB/s, and 32 GB/s for Superdome 16-way, Superdome 32-way, and Superdome 64-way systems, respectively.

ECT - 1 8689 A CPL - AC

In addition to the interface logic, the cell controller ASIC maintains cache coherency throughout the system. The cell controller ASIC supports the PA-8700 processor and can support future PA-RISC processors.

The processor-dependent hardware, or PDH, is the module that provides the cell-local resources required to reset a cell and bring it up to a point where it can join other cells and boot the operating system. PDH contains the system boot firmware, which is also used at runtime.

memory controller ASIC

The memory controller ASIC is also part of the Superdome system chip set. Its primary function is to multiplex and demultiplex data between the cell controller ASIC and the SDRAMs in the memory subsystem. When the cell controller ASIC issues transactions on the memory interface command bus, the memory controller ASIC buffers those read transactions and returns the data as soon as it is available.

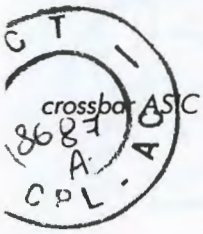
Note that only the data portion of the memory subsystem goes through the memory controller ASIC. All address and control signals to the DIMMs are generated by the cell controller ASIC and sent directly to the DIMM via the memory interface address bus.

The memory subsystem is a dual-ported implementation. It supports memory DRAM fault tolerance, where a discrete SDRAM chip can fail without compromising data integrity. The memory subsystem provides 4 GB/s of bandwidth to the cell controller ASIC and minimizes the overhead typically associated with directory coherency. What's more, the memory subsystem enjoys a very low latency for cell-to-local-memory access: as low as 200 ns average idle latency at 250 MHz load-to-use.

the crossbar backplane

Each crossbar backplane contains two sets of two crossbar ASICs that provide a non-blocking connection between eight cells and their associated memory and I/O. Each backplane cabinet can support up to eight cells or 32 processors (in a Superdome 32-way). Two backplanes can be linked together with a flex cable to produce a cabinet that can support up to 16 cells or 64 processors (Superdome 64-way).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 817
Doc. 3698



The crossbar ASIC is yet another part of the Superdome system chip set. It implements a high-performance 8-port non-blocking crossbar and the 500 MHz crossbar link protocol. All ports are functionally and electrically identical. Superdome's fabric is a fully connected crossbar mesh with four crossbar ASICs and four cells per crossbar ASIC. Like the cell controller ASIC, the crossbar ASIC has truly impressive scale. HP believes it to be the world's second largest ASIC, with 18 million transistors and six layers of metal, using copper technology.

A very important aspect of the crossbar mesh is that all links have the same bandwidth and latency—which is key to maximizing overall bandwidth and minimizing overall latency. Cell-to-crossbar and crossbar-to-crossbar communication occur at the same speed; there are no excessive latency penalties for going remote. In addition, Superdome's memory interleaves across cells first, then across memory banks. This interleaving scheme tends to balance out memory traffic across all the links.

The crossbar mesh implements a global point-to-point packet filtering network. This mesh features an extremely high level of integrity, with each crossbar port fully independent. The crossbar mesh has dedicated paths for data and control, and each port can be reset, assigned, or reconfigured fully independent of other ports. Superdome's crossbar mesh is an excellent foundation for resource isolation.

The crossbar ASIC offers several features that contribute to Superdome's high performance:

- Support for scaling up to a 256-way coherent shared memory system.
- 250-MHz operation
- 500-MT/s link speed
- Support for two interleaved channels on link protocol.
- Support for double-length data packets for Itanium Processor Family mode.
- Performance counters to enable software tuning.

Each port on the crossbar ASIC is 6.4 GB/s. These ports provide a high-throughput path to cells and other crossbar ASICs:

- Four ports connect to the four cells that reside on the crossbar ASIC (one port per cell).
- Three ports connect to the remaining three crossbar ASICs (in a Superdome 64-way). The remaining port may connect to another system to form a multi-node configuration (Scalable Computing Architecture) that is currently not supported.

1 8691 A CPL - AC

the cell board

A cell, or cell board, shown in **figure 4**, is the basic building block of a Superdome system. Each cabinet can contain up to eight cell boards, which are plugged into the backplane of the cabinet.

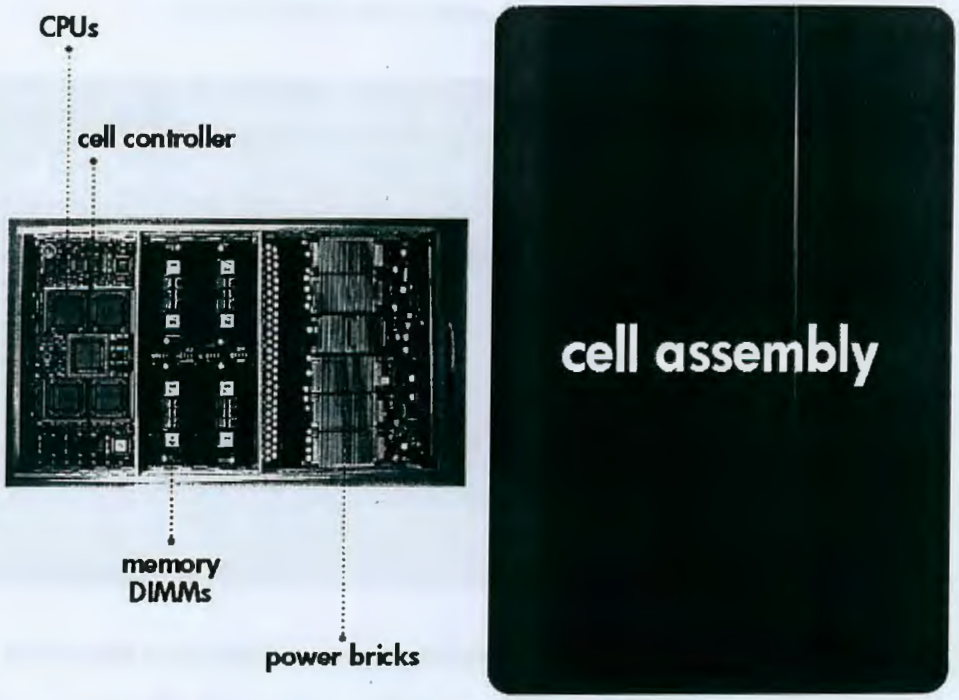


figure 4: superdome cell board layout

Each cell board is a self-contained unit, with a symmetric multiprocessor (SMP), main memory, and all necessary hardware:

- CPUs (up to 4 processors)
- Cell controller ASIC (application-specific integrated circuit)
- Main memory DIMMs (up to 16-GB RAM in 2-GB increments, using 128-Mbit SDRAMs)
- Power bricks (power converters)
- Data buses
- Optional link to 12 PCI I/O slots

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 818
Doc. 3698

Figure 5 illustrates the cell board architecture. The cell has a peak memory bandwidth of 4 GB/s. A connection to a 12-slot PCI card cage is optional for each cell, and the peak bandwidth of this link is 2 GB/s. Bandwidth to the crossbar is 8 GB/s.

Except for the DIMM connections, most links in the cell are point-to-point connections. All links are protected by parity (processor link, I/O link) as well as ECC—error checking and correcting (all memory data and fabric ports).

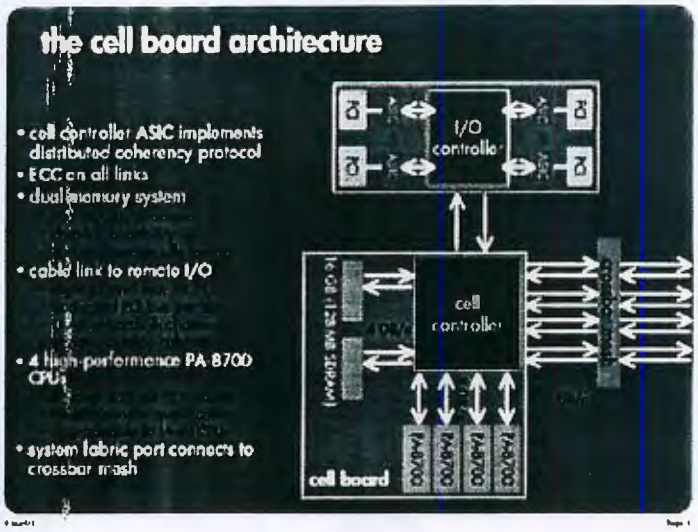


figure 5: superdome cell board and interconnect architecture

In the future, cell boards will support up to 32 GB of memory using 256-Mbit SDRAMs.

processors

The initial release of the Superdome uses ECC-protected PA-8700 processors running with a core frequency of 750 MHz and an on-chip cache of 2.25 MB. Future Superdome implementations will support Itanium Processor Family processors as well as future PA-RISC processors.

cell controller ASIC

Residing on the cell board, the cell controller ASIC (application-specific integrated circuit) is part of the Superdome system chip set. It coordinates memory between the major components of a cell board and determines if a request requires communication with another cell or with the I/O subsystem. HP believes that this cell controller ASIC is the largest ASIC in the world: it has some 24 million transistors and six layers of metal, using copper technology.

The cell controller ASIC has five major interfaces:

- 2 ports to memory controllers (DIMMs)
- 4 ports to processors (one dedicated port per processor for the highest possible performance)
- 1 port to the crossbar, through which all communication to other cells flows
- Processor-dependent hardware (PDH)
- 1 port to the I/O bus, which connects the cell to an I/O subsystem

3693
A
CPL - AC

Features of the Superdome cabinets include:

- **Front and rear servicing:** You can service Superdome cabinets from the front and rear of the cabinet. This lets you arrange the cabinets of your Superdome system in the traditional row fashion found in most computer rooms.
- **Sized for easy installation:** Installation is no problem—the width of the Superdome cabinet allows entry through most doorways without disassembly.
- **Hot-swappable filters:** The intake air to the cell boards is filtered, helping to keep these boards clean and operational longer. You can remove the filter for cleaning or replacement while the system is fully operational.
- **External status display:** A status display on the outside of the front and rear doors of each cabinet allows maintenance personnel and HP field engineers to determine the basic status of each cabinet without opening any cabinet doors.

superdome system architecture

Superdome is a ccNUMA (cache-coherent, Non-Uniform Memory Access) system. And Superdome presents an SMP (symmetric multi-processing) programming model to the operating system by enabling any processor to have access to any byte of memory anywhere in the system. In fact, Superdome is the first mission-critical UNIX system to exploit distributed processors and memory. Here's why:

- **Usable bandwidth scales with system size, thanks to two important design features:**
  - **Superdome's coherency scheme:** Unlike some UNIX systems, which rely on snoop-based coherency that results in bottlenecks (large, flat latencies and bandwidth starvation) in high-end configurations, Superdome sidesteps the overheads usually attributed to directory coherency.
  - **Superdome's topology:** Superdome implements a point-to-point global packet switch for a communication fabric that is very well balanced across processor, memory, and I/O traffic.
- **Large physical memory with extremely low latency:** At first release, Superdome uses 128Mbit SDRAM technology and provides 2X DRAMs per processor, yielding a maximum memory of 256 GB. In the future, Superdome will be the first system in the industry to surpass 1 TB memory capacity. And even with these high amounts of memory, the latency growth from 4 to 64 processors is only 1.6X (60% growth), which is extremely flat.
- **High I/O bandwidth and connectivity:** Superdome provides a high degree of I/O connectivity while preserving bandwidth. There are 192 PCI cards in the system, each with its own dedicated PCI bus; at the adapter level, this aggregates to 64 GB/s of raw bandwidth. The I/O bandwidth available between the system core (processors and memory) and the I/O controllers is roughly 30 GB/s.
- **Large number of high-performance processors:** Superdome provides 64 PA-8700 processors—and these are the highest-performance processors in the industry. (Compare this system to those from other UNIX system vendors; while the systems may provide up to 64 processors, their uniprocessor performance does not match that of PA-8700.)
- **True hardware isolation of system resources:** Processors, memory, and I/O resources are truly isolated from each other in order to provide flexibility in system usage. This means:
  - Great SMP performance to attack large single workloads.
  - Hardware-enforced isolation of resources, coupled with great single-system high availability and manageability features for a strong consolidation platform.

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 3698
Doc.

modular architecture

Superdome's architecture is modular, with components that can be used to construct several different server-class computer products based on PA-8700 processors. (Processor upgrades beyond PA-8700 require a new version of the cell board.) Such modularity helps provide investment protection—you can simply add or change components as system requirements change.

The Superdome platform supports a variety of system configurations from 1 to 64 processors. The system is extremely flexible and has a cell-based hierarchical crossbar architecture that can be configured as one large symmetric multiprocessor or as several independent nPartitions.

You can choose from three models in the Superdome server family. The largest is an 8- to 64-processor system with a scalable memory and I/O subsystem. In a Superdome system, any processor on any nPartition can directly address any byte of memory on any nPartition, through processor-issued load or store instructions.

There are three basic components in the Superdome system architecture: the cell or cell board, the crossbar backplane, and the PCI-based I/O subsystem. **Figure 3** is an illustration of this architecture.

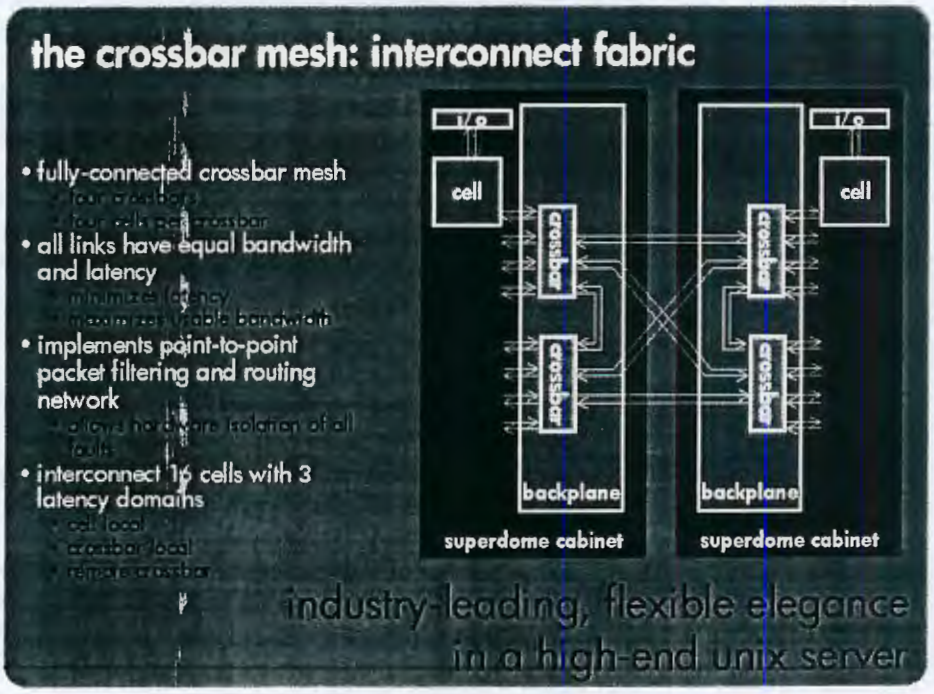


figure 3: superdome's hierarchical crossbar architecture

8695 A. CPL - AC

superdome hardware overview

You can choose Superdome in several different configurations, with capabilities from 2-way multiprocessing all the way to 64-way. Depending on the model, Superdome comes in one or two cabinets. Here's a summary of Superdome hardware:

	superdome 16-way	superdome 32-way	superdome 64-way	superdome I/O expansion (see note 1)
4-CPU cell boards (hot-swap capability offered with HP-UX releases after 11i)	1–4	1–8	8–16	
CPUs	1–16	1–32	8–64	
memory (with 512 MB DIMMs)	4–64 GB	8–128 GB	16–256 GB	
12-slot I/O card cages	4	4/8	8/16	6
hot-swap PCI I/O slots	48 slots (32 33-MHz slots, 16 66-MHz slots)	48/96 slots (64 33-MHz slots, 32 66-MHz slots)	96/192 slots (128 33-MHz slots, 64 66-MHz slots)	72
hot-swap redundant power supplies (N+1 included)	4	6	12	2
I/O fans	6	6	12	4 per I/O chassis enclosure (max 12)
hot-swap redundant fans (N+1 included)	4	4	8	
nPartitions	4	4/8	8/16	
crossbar bandwidth (peak)	16 GB/s	32 GB/s	64 GB/s	
2X PCI I/O bus bandwidth	266 MB/s	266 MB/s	266 MB/s	
4X PCI I/O bus bandwidth	533 MB/s	533 MB/s	533 MB/s	
cell controller to I/O subsystem bandwidth (peak)	2.0 GB/s	2.0 GB/s	2.0 GB/s	
I/O bandwidth (peak)	8 GB/s	16 GB/s	32 GB/s	
cell controller to memory subsystem bandwidth (peak)	4 GB/s	4 GB/s	4 GB/s	
memory bandwidth (peak)	16 GB/s	32 GB/s	64 GB/s	
average memory load-to-use latency:				
4-CPU	235 ns	235 ns	235 ns	
8-CPU	266 ns	266 ns	266 ns	
16-CPU	296 ns	296 ns	296 ns	
32-CPU	N/A	336 ns	336 ns	
64-CPU	N/A	N/A	360 ns	
average idle memory latency (system is idle):				
4 CPU	174 ns	174 ns	174 ns	
8 CPUs	208 ns	208 ns	208 ns	
16 CPUs	228 ns	228 ns	228 ns	
32 CPUs	N/A	261 ns	261 ns	
64 CPUs	N/A	N/A	275 ns	
operating system	HP-UX 11i	HP-UX 11i	HP-UX 11i	HP-UX 11i
average power dissipation	3,756	5,740	11,480	
number of cabinets	1 (left)	1 (left)	2 (1 left, 1 right)	1 Rack System E Expansion
dimensions:				
height	1.96 m (77.2 in)	1.96 m (77.2 in)	1.96 m (77.2 in)	1.96 m (77.2 in) 1.60 m (63.0 in)
width	762 mm (30 in)	762 mm (30 in)	1524 mm (60 in)	610 mm (24 in)
depth	1220 mm (48 in)	1220 mm (48 in)	1220 mm (48 in)	1220 mm (48 in)

Note 1: For I/O expansion up to 168 slots, one Expansion Cabinet (holds up to 6 I/O card cages) is required. For I/O expansion up to 192 slots, two Expansion Cabinets are required. Any remaining space in the I/O Expansion Cabinets can be used to store peripherals. Both the 1.96m and 1.6m heights are available for the I/O Expansion Cabinet.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 820
Doc. 3698

For maximum flexibility in configuring the data center, a Superdome system has up to four different types of cabinet assemblies:

- Superdome 16-way and Superdome 32-way systems are single-cabinet configurations with one Superdome left cabinet. The Superdome cabinet contains all of the processors, memory, and core devices of the system. It also houses up to 48 PCI I/O cards or 4 I/O chassis.
- The Superdome 64-way system is a dual-cabinet configuration with one Superdome left cabinet and one Superdome right cabinet. Together, the two cabinets contain all of the processors, memory, and core devices of the system. The dual-cabinet configuration houses up to 96 PCI I/O cards or 8 I/O chassis.
- An optional I/O Expansion Cabinet is added if the required number of PCI I/O cards exceeds the number of PCI I/O cards that can be accommodated in a 32-way or 64-way configuration.

the superdome cabinet

Figure 2 shows the physical layout of a Superdome 32-way cabinet. At the top of the cabinet, hot-swappable main fans are installed after the cabinet arrives at the customer site. Below these fans is a cage for the eight cell boards on which processors and memory DIMMs reside. For all HP-UX 11 releases after 11i, these cell boards support hot-swap capability, so you can change them without bringing down the system.

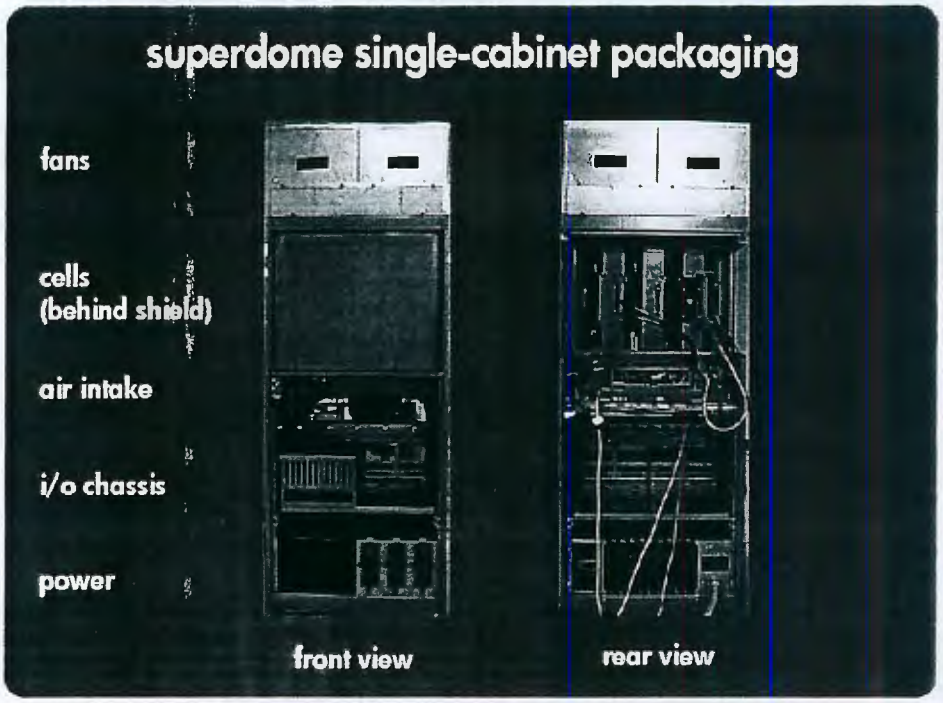


figure 2: front and rear views of superdome 32-way cabinet

Directly below the cell boards is the main air intake, and below that are two I/O chassis. Each I/O chassis holds an I/O card cage. Redundant power supplies are at the bottom of the cabinet. The Superdome family does not use electric plugs; instead, –48 Vdc power is hard-wired to each cabinet. There are two redundant power inputs so that the system can be powered up via two different power grids. An opening in the side of the cabinet allows two Superdome 32-way cabinets to be cabled together to constitute a Superdome 64-way.

8697
A.
CPL - AC

The HP Server product line represents the most scalable range of computing available today. These systems feature:

- *Application compatibility and portability* across the product line, permitting users to select the best platform at the appropriate price point without worry about whether applications will run on it.
- *The highest uniprocessor performance* in the industry, providing reduced time-to-solution through parallelism and increased throughput through multiprocessing, in all environments.
- *Unmatched scalability*, providing the best price/performance over the entire range of products and protecting customers' investments in hardware and software.
- *A consistent programming model*, presenting the same application programming environment regardless of the systems' performance levels; this greatly increases the number of available "off-the-shelf" third-party applications and reduces porting and development costs.
- *Leading-edge utility pricing models* (Pay per Use, Capacity on Demand, and Pay per Forecast), allowing customers to better align their IT costs with revenues as their technology usage fluctuates over time.

the need for "big iron"

Some applications simply need the maximum amount of performance and availability. For instance, in the "Internet powerhouse"—the data center where transaction processing is handled and where the backbone of mission-critical applications runs—you'll want the best servers available to keep those applications running and meeting quality-of-service goals on a 24 x 7 basis. The Internet powerhouse, along with other workload types such as OLTP with database engines, data mining, and customer relationship management, are best handled by "big iron," top-of-the-line computers that also combine security, scalability, flexibility, capacity, and manageability. That's where Superdome fits in.

introducing superdome enterprise servers

Superdome is the latest addition to the HP family of HP-UX Enterprise Servers, and it extends the capabilities of this server family in several important areas:

- Scalabilty
- Performance
- Capacity
- Availability
- Flexibility
- Investment protection
- Manageability

As a high-end platform for the Internet data center, Superdome is uniquely able to address your requirements, even as those requirements change over time. This capability is based on Service Level Agreement (SLA) features, hard and soft partitions, scalability up to 64 industry-leading processors, and multiple operating environments (OEs). Superdome is also the *first high-end server family to be upgradable to Itanium™ Processor Family (IPF) processors!*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 821
Nº 3698
Doc.

top-of-the-line performance and capacity

Superdome is the best choice for the Internet powerhouse because it greatly extends the capabilities of HP Servers at the high end:

- High-performance RISC processor (PA-8700)
  - 750-MHz, 4-way superscalar (3.0 GFLOPS)
  - 0.18 micron copper silicon-on-insulator CMOS process
  - Data prefetching capability
  - Large on-chip cache (2.25 MB)
  - Upgradable to IPF processors
- Increased memory subsystem performance
  - Increases peak memory bandwidth to 64 GB/s per 64-way system
  - Higher density system packaging provides 256 GB per 64-way system
- Doubled processor capacity compared to V-class
  - Configurations available from 2 to 64 CPUs
- Doubled I/O interface performance; more than doubled I/O bandwidth
  - 64-bit 33 MHz (2x) industry-standard PCI
  - 64-bit 66 MHz (4x) industry-standard PCI
  - Sixteen 2.0 GB/s I/O channels (32 GB/s per 64-way system)
  - Increased number of PCI slots (up to 192)

availability features for maximum uptime

Mission-critical applications are no problem for Superdome. This family of servers has the increased system reliability and availability necessary to provide *maximum uptime*. It has improvements in system quality, resiliency, and fault management; and it provides support for MC/Serviceguard in a Superdome cluster.

flexibility with partitions

Superdome supports the HP Partitioning Continuum, allowing both hard and soft partition. In fact, Superdome can be configured as one large symmetric multiprocessor or as several independent hard partitions, known as nPartitions. These nPartitions can provide hardware isolation and complete software isolation, and you can dynamically resize partitions for the highest degree of flexibility. Partitions allow Superdome to reach new heights in availability and scalability, too.

investment protection, with support for PA-RISC or IPF processors

At first release, Superdome supports PA-RISC processors, with support for IPF processors coming soon. This makes it the logical choice not only for your present and future high-end computing needs, but also for ensuring investment protection in the years to come.

better manageability

Superdome includes all-new management features coupled with tested management software and technologies, all designed to increase your control while reducing administrative overhead. With tools such as the Superdome Support Management Station (SMS), Partition Manager, and Servicecontrol suite at your fingertips, you'll find that a Superdome system is extremely easy to manage.

hp-ux 11i, the proven 64-bit operating environment

HP-UX 11i is an operating environment specifically focused on the needs of both online economy companies and traditional economy concerns. Superdome runs this industry-leading operating environment.

HP-UX 11i is an Internet-focused version of HP's 64-bit operating system that enjoys the industry's greatest support from independent software vendors. In fact, you can choose from more than 16,000 applications, including native 64-bit versions of all major databases and leading enterprise resource planning (ERP) applications. The widely supported 64-bit HP-UX operating system is compatible with the full line of HP Servers.

8699
A.
CPL - AC

SMS installation
SMS functional capabilities 27
partition manager 27
servicecontrol suite 27
superdome and hp-ux 11i **28**
features of hp-ux 11i 28
hp-ux 11i operating environments 28
entry-level hp-ux 11i 29
hp-ux 11i enterprise 29
hp-ux 11i mission-critical 29
the rest of the superdome story **29**
the always-on infrastructure and superdome 29
peripherals and superdome 29
mass storage and superdome 29
conclusion **29**
availability 29
capacity 30
connectivity 30
security 30
manageability 30
for more information **30**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 822
Doc. 3698

abstract

Superdome is the high-end UNIX® server in the HP Server product family. It's designed to deliver the performance, availability, capacity, security, and manageability needed for the "mission-critical Internet" and other compute-intensive applications. In this white paper, you'll learn about the architecture, system software, and management tools of the Internet-ready HP Superdome Enterprise Server.

the hp 9000 enterprise server product line

First, let's look at the overall HP Server product lineup. These servers address the major computing challenges that customers face today. Running the powerful HP-UX operating environment (Hewlett-Packard's version of UNIX), HP Enterprise Servers are especially suited to the demands of the Internet, online transaction processing (OLTP), system consolidation, large decision support systems, and compute-intensive technical applications.

As shown in **figure 1**, the HP Server line is extremely comprehensive, with products ranging from entry-level products to high-end platforms. And now, added to the existing A-, L-, and N-class servers, Superdome is positioned as the family's most powerful high-end platform.

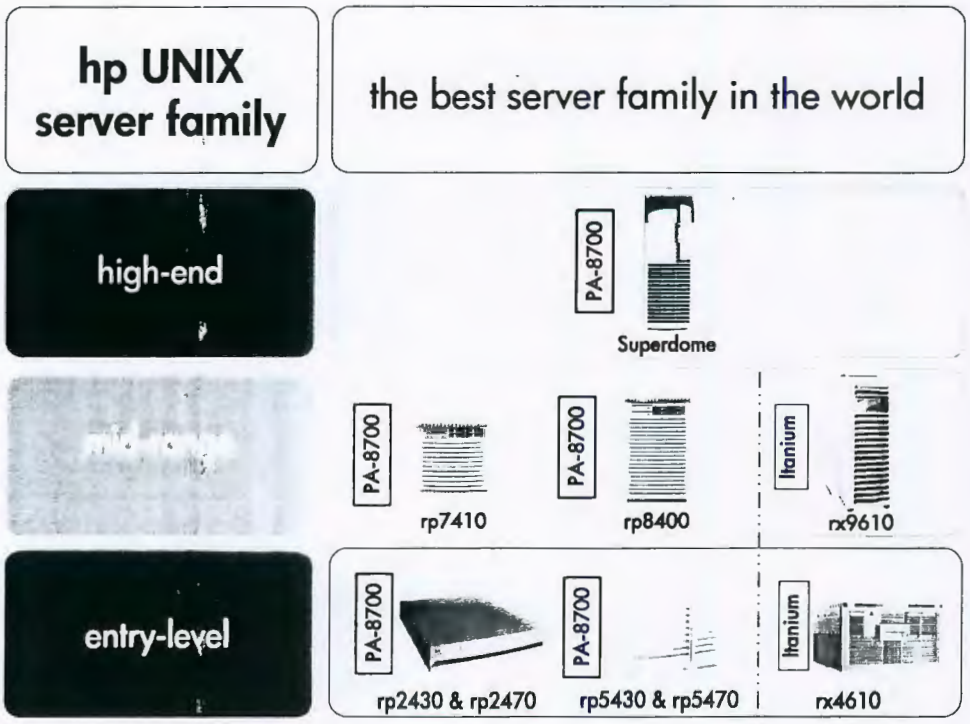


figure 1: the hp server family

ECT
1 8701
A.
CPL - AC

meet the hp superdome servers

May 2002

a white paper from Hewlett-Packard Company

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc.

T
CPL

table of contents.

abstract 3
the hp 9000 enterprise server product line 3
the need for "big iron" 4
introducing superdome enterprise servers 4
top-of-the-line performance and capacity 5
availability features for maximum uptime 5
investment protection, with support for PA-RISC or IPF processors 5
better manageability 5
hp-ux 11i, the proven 64-bit operating environment 5
superdome hardware overview 6
superdome hardware 7
the superdome cabinet 7
superdome system architecture 8
modular architecture 9
the cell board 10
processors 11
cell controller ASIC 11
memory controller ASIC 12
the crossbar backplane 12
crossbar ASIC 13
memory and backplane latencies 14
the I/O subsystem 15
superdome: performance and scalability 16
system bandwidth 16
scalability 16
superdome: high availability 16
superdome: system reliability 17
supportability 17
hardware inventory in support tools manager 18
support management station 18
high availability observatory 18
repairability 19
n+1 CPUs with iCOD 19
n+1 fans, power supplies, backplane DC/DC converters 20
dual power sources 20
online addition and replacement (OLAR) of PCI I/O cards and chassis 20
online addition and replacement of cell baards 20
online addition of nPartitions 20
mc/serviceguard- in-a-box 20
superdome: investment protection 20
microprocessor roadmap 21
binary compatibility for across PA-RISC 22
binary compatibility for Itanium Processor Family 22
upgrading a superdome system 22
superdome partitioning 22
the hp partitioning continuum 23
hyperplex: hard partitions with multiple nodes 23
nPortitions: hord partitions within o node 23
virtual partitions 24
resource portitions 24
how nPartitions work 24
uses for nPartitions 24
increased systems utilization 25
increosed flexibility via support of multiple environments 26
increosed uptime 26
increosed scalability 26
superdome: ease of management 26
superdame support management station 26

Apêndice IM

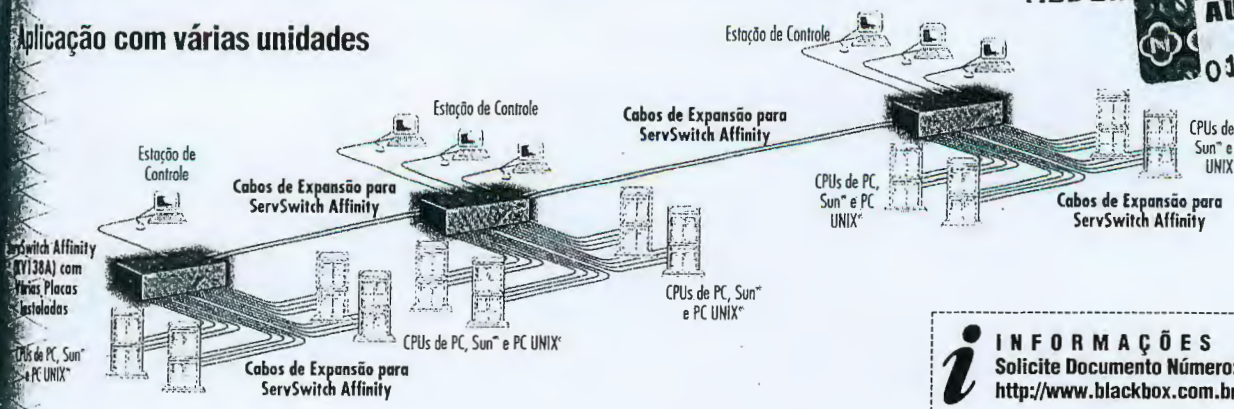
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 824
Nº 3698
Doc.

BLACK BOX
NETWORK SERVICES

1000 CPUs para você e até 16 consoles!

REGISTRO C... ALDEIA... RUERI - SP
Colégio Notarial do Brasil - S.P.
AUTENTICAÇÃO
0109A 61277654
1 8666 A- CPL - AC

Aplicação com várias unidades



INFORMAÇÕES
Solicite Documento Número: 22921
http://www.blackbox.com.br

ESPECIFICAÇÕES

Estrutura — Chassi de aço
Suporte a CPU — IBM™ PC e compatíveis, PS/2™, Sun™ e a maioria dos PC UNIX™ (RS/6000™, HP9000™, SGI, DEC™ Alpha e outros); conectado em cascata para até 1000 CPUs
Configuração Máxima por Chassi — (4) usuários, (1)...Js, (1) Placa de Expansão
Suporte a Mouse — Microsoft™ Serial ou PS/2, Sun Microsystems™ e compatíveis
Resolução de Vídeo — Até 1280 x 1024
Aprovação pela CE — Sim
Conectores — Todos os chassis: (1) alimentação IEC 320;
KV132A: (10) DB25 F, (2) RJ-11;
KV134A: (20) DB25 F, (4) RJ-11;
KV1300C: (4) DB25 F;
KV1301C: (5) DB25 F;
KV1305C: (2) DB15 F, (2) DB15 M;
Cabos de Expansão: (1) DB15 F, (1) DB15 M
Indicadores — Chave de alimentação retro-iluminada
Alimentação — 90–264 VCA, 47–63 Hz, 40 watts, automática
Dimensões — Chassi ServSwitch Affinity:
13,3A x 42,4L x 17,8P cm
KV1300C, KV1301C, KV1305C: 35,3 x 12,2 cm;
KV1304C: 10,2 x 7,6 cm
Peso — KV130A: 4,9 kg;
KV132A: 5,6 kg;
KV134A: 6,5 kg;
KV1300C–KV1301C: 0,4 kg;
KV1304C: 0,1 kg;
KV...: 0,2 kg,
KV...: 6,9 kg
...DO PROTECTION™ — 2 Anos

Item	Código	Preço
Peça o chassi pré-configurado adequado para sua aplicação...		
ServSwitch Affinity		
2 Usuários x 8 CPUs(inclue 1 Placa terminadora KV1304C)	KV132A	**4.102,00**
4 Usuários x 16 CPUs(inclue 1 Placa terminadora KV1304C)	KV134A	**7.330,00**
1 Usuário x 16 CPUs(inclue 1 Placa de expansão KV1305C)	KV131A	**7.330,00**
...ou faça sua própria configuração. Primeiro adquira o...		
Chassi de Expansão ServSwitch Affinity(Não placas inclusos)		
Chassi Arquitetura de 4 usuários (4 Slots + 1Slot de Expansão)	KV130A	**1.748,00**
Chassi Arquitetura de 8 usuários (4 Slots + 1Slot de Expansão)	KV138A	**5.803,00**
Chassi Arquitetura de 16 usuários (4 Slots + 2 Slots de Expansão)	KV139A	**7.344,00**
...Depois acrescente as placas apropriadas...		
ServSwitch Affinity Cards		
0 Usuários x 4 CPUs	KV1300C	**1.346,00**
1 Usuários x 4 CPUs	KV1301C	**1.812,00**

Verifique abaixo quais são os conectores que as suas CPUs/ Servidores possuem, depois veja os códigos dos cabos necessários nas páginas correspondentes...(Utilize tamanho máximo 30m).
Peça 1 cabo para cada console e 1 cabo para cada CPU conectada.

Cabos CPU/Server para ServSwitch

PC PS/2	Plataforma	Monitor	Teclado	Mouse
	PS/2™	HD15	Mini DIN 6 Pinos	Mini DIN 6 Pinos

AT	Plataforma	Monitor	Teclado	Mouse
	AT™	HD15	DIN 5 Pinos	DB9

Veja os códigos na pág. 512.

Sun 13W3	Plataforma	Monitor	Teclado / Mouse
	Sun 13W3	13W3	Mini DIN 8 Pinos

VGA	Plataforma	Monitor	Teclado / Mouse
	Sun VGA	HD15	Mini DIN 8 Pinos

Veja os códigos na pág. 512.

Item	Código	Preço
Se você estiver montando uma configuração de chassi único com o KV130A, peça a...		
ServSwitch Affinity Placa Terminator	KV1304C	**52,00**
Para aplicações com vários chassis, adicione a placa de expansão adequada...		
Placa de Expansão ServSwitch Affinity, 4 Usuários	KV1305C	**872,00**
Placa de Expansão ServSwitch Affinity, 8 Usuários/16 Usuários	KV1306C	**2.541,00**

OBS: No KV132A, KV134A, KV130A utilize (1) KV1305C. No KV138A utilize 1x KV1306C. No KV139A utilize 2x KV1306C

Se você quiser instalar seus chassis em rack, peça o kit apropriado para (KV138A e KV139A)...

Kits ServSwitch Affinity para Rack		
19"	RMK19A	**39,00**
23"	RMK23A	**51,00**
24"	RMK24A	**51,00**

Item	4 Usuários	Preço	8 /16 Usuários	Preço
Para conectar múltiplos chassis, peça...				
Cabos de Expansão ServSwitch Affinity				
3,0 m	KV140010	**107,00**	KV180010	**115,00**
6,0 m	KV140020	**146,00**	KV180020	**157,00**
10,6 m	KV140030	**Consulte**	KV180035	**225,00**
15,2 m	KV140050	**247,00**	KV180050	**265,00**
30,4 m	KV140100	**438,00**	KV180100	**471,00**

OBS.: Para expandir os Chassi de 4 usuários utilize 2 cabos KV14XXXX. Para expandir os Chassi de 8 usuários utilize 4 cabos KV18XXXX. Para expandir os Chassi de 16 usuários utilize 8 cabos KV18XXXX.

AO LIGAR TENHA SEMPRE EM MÃOS O CGC DA SUA EMPRESA E O SEU CPF.
PARA PEDIDOS, LIGUE: (011) 55154001
03/2... 501 CM
EMI... CORREIOS
Fls Nº 825
Nº
Doc. 3698

Nº
Fls. Nº 3698
Doc.

Apêndice IN

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 827
3698
Doc.

ECT - CPL - AC 18663 A.

• Humidity (non-condensing)		condensing	
	Non-operating		-40 to 85° C
	Maximum Wet Bulb Temperature	101.7° F	38.7° C
Acoustic Noise	Idle (Fixed Disk Drives Spinning)	L WAd (BELS)	6.5
		L pAm (dBA)	47.3
	Operating (Random Seeks of Fixed Disks)	L WAd (BELS)	6.7
		L pAm (dBA)	50.3

Top of page

This page was updated on February 19, 2003

Comments about this page

Privacy and Legal Statement

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 828
Nº 3698
Doc.

1 8664 A
CPL - AC

ProLiant DL740

Specifications

Category	Specification	U. S.	Metric
Physical Dimensions (Rack)	Height	7.00"	17.78 cm
	Depth	28.7"	72.90 cm
	Width	17.5"	44.45 cm
Weight (Rack)	No hard drives installed, two power supplies	105 lbs.	47.63 kg
Input Requirements	Rated Input Voltage	100 to 120 VAC/200 to 240 VAC (lowline/highline)	
	Rated Input Frequency	47 to 63 Hz (lowline/highline)	
	Rated Input Current	12A at 100 VAC/8A at 200 VAC (lowline/highline)	
	Input Power	1142W/1570W (lowline/highline)	
Power (watts) per Power Supply	Rated Steady State Power	800W/1100W (lowline/highline)	
	Maximum Peak Power	800W/1100W (lowline/highline)	
	Heat Dissipation (BTU's)	1555 Watts [5309 BTU/hr] (System is configured to draw maximum power)	
Environmental Requirements • Temperature	Operating	40° to 110°	5° to 43°C (End use system maximum ambient of 35°C, plus a maximum of 8°C due to rack effect)
	Non-operating	-40° to 185°	-40 to 85° C
	Shipping	5% to 95% relative humidity, non-condensing	
Environmental Requirements	Operating	5% to 95% relative humidity, non-	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 829
Doc. 3698

Apêndice IO

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 830
Doc. 3608

8662
A.
CPL - AC

EMBEDDED DISPLAY GRAPHICS

RAGE™ XL Product Snapshot

Delivering strong 2D/3D/video acceleration, RAGE™ XL is ideal for situations where small package sizes are crucial, ease of integration is a must and upgrade ability is a necessity

Package Specifications

- ***Package, Size:*** 272 BGA, 27mm x 27mm

Graphics Processor Specifications

- ***Process technology, Core Voltage:*** 0.25um, 2.5V
- ***Graphics Clock:*** 83 MHz

Memory Specifications

- ***Maximum Memory Configuration:*** 8MB External Memory
- ***I/O Type, VDDC:*** 3.3V (LVTTL)
- ***Memory Clock, Max Memory Path:*** 125 MHz, 64 bit width

Bus Specifications

- ***AGP bus support/ PCI bus support::*** AGP 2X (3.3V)/ PCI 2.2

Outputs

- ***CRT:*** Triple 8-bit palette DAC, 230MHz
- ***Integrated TMDS:*** DVI, DFP and VESA P&D interface
- ***Support for 24bit TTL***

Resolution Support

- ***Max 2D/3D resolution***: 1600x1200
- ***Max color depth***: 16.7M Colors
- ***TMDS:*** 1024x768

Driver Support

- Win 98/ME/NT/2000/XP, Linux (Please see your technical contact for alternate OS support)

Copyright 2003, ATI Technologies Inc. All rights reserved. ATI, MOBILITY, RADEON, RAGE, POWERPLAY and HYPER Z are trademarks and/or registered trademarks of ATI Technologies Inc. All other company and/or product names are trademarks and/or registered trademarks of their respective owners. Features, performance and specifications may vary by operating environment and are subject to change without notice. Products may not be exactly as shown. Printed in Canada. 05/03 117-40186-10

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 831
Nº Doc. 3698

Apêndice IP

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 832
Doc 3698

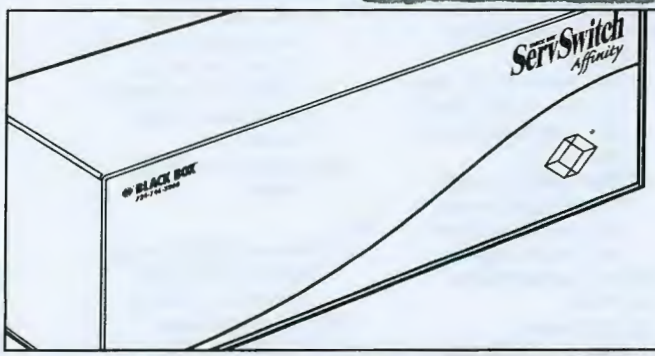
8661

BLACK BOX® NETWORK SERVICES

© 2001. All rights reserved.
Black Box Corporation.

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

SERVSWITCH™ AFFINITY



Affordable many-to-many multiplatform KVM switching.

Key Features

- ***As many as 16 users have keyboard/mouse/video control over as many as 1024 PC, Sun, RS/6000, SGI, HP, and/or Alpha computers.***
- ***With additional converters, also supports Apple computers.***
- ***Easily expandable with plug-in Port Cards and flexible cabling.***
- ***Free lifetime firmware upgrades.***
- ***Supports video resolutions up to 1280 x 1024.***
- ***High levels of security, including passwords and access profiles.***
- ***Controlled through on-screen display, with additional keyboard commands and a terminal-based serial-port options menu.***
- ***Some models have redundant power supplies.***

Is your server room growing by leaps and bounds? Wouldn't it be nice to have a keyboard/video/mouse-switching system that could keep up with all the hardware, all the users, the constant changes, and the realities of your budget?

Our ServSwitch™ Affinity could be the one. It will support most major hardware platforms, including IBM® PS/2®, PC/AT®, and RS/6000®; Sun®; SGI™; HP® 700 and 9000 series; and Compaq® Alpha™. IBM type computers can use any keyboard mode and any of a variety of mouse types. Video can be any of several types at up to 1280 x 1024 resolution. With additional adapters, you can attach Apple® Macintosh® CPUs too—see **"What else you might need"** on page 4.

You can attach as many as 16 computers to a single unit or 1024 computers to a daisychained Affinity system. Either way, you can also attach up to 4, 8, or 16 independent users; more users can be connected, but they'll have to contend for access.

Here's how it works: Each ServSwitch Affinity has four slots for Port Cards. 0 x 4 Port Cards (product code KV1300C) have four CPU (computer) ports and a serial port only; 1 x 4 Cards (KV1301C) also have a KVM (user) port.

The Affinity chassis also has a fifth, top slot used for expansion purposes; the 16-User models have a matching sixth, bottom slot. 4-User models ship with a Terminator Card (KV1304C) installed in the expansion slot; you can swap in a 4-User Expansion Card (KV1305C) if you'll be daisychaining the Affinity. 8- and 16-User models, which are designed to be part of a daisychain, come without anything installed in the expansion slot(s). You need to purchase and install an 8-User Expansion Card (KV1306C) for each slot in order for the unit to work.

The only difference between the three 4-User Affinity models with single power supplies is which Cards they're preinstalled with; see the start of **"Ordering Information"** on page 5 for a list of which Cards come with each model.

You can add capacity to your Affinity system at any time by installing Port Cards in vacant slots or adding more chassis to a daisychain.

The Port Card's serial ports are used for terminal-based initial system configuration; they are also used to upgrade the Affinity's firmware (upgrades are free for the lifetime of the Affinity!).

The ServSwitch Affinity's main controls are its on-screen menus (with a full range of configuration and operating functions). These menus are augmented by a number of keyboard commands.

For added security, the Affinity supports password-protected access groups. Computers can belong to multiple groups, but users can only belong to one. Users will only be able to access the computers in their group.

When users do access computers, they'll have one of four assigned access levels: view only (no keyboard/mouse control), share (view access until current user becomes inactive, then add keyboard and mouse), control (sole control but others can view), or private (sole control, no one else can interrupt or view).

For mission-critical applications, we offer models of the Affinity with dual, redundant power supplies. If one power supply ever fails, the other can take on the entire load until a replacement supply can be installed.

6/26/2001 #22921

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 833
Nº Doc. 3698

Specifications

Hardware Required: Monitor that supports your computers' highest video standard; in multiplatform applications, should be multisync model that can video from either composite sync or separate horizontal/vertical sync signals

Compliance: CE, FCC Part 15 Subpart J Class A, IC Class/ classe A

Standards:
- With original Serv cabling: VGA (color or monochrome/page white) video;
- With original Serv cabling (minimal) or coaxial cabling (recommended): SVGA and (with KV99MA adapter) Mac video;
- With coaxial cabling: XGA (color or monochrome), Sun, RS/6000, or SGI video

Interfaces:
- On CPU ports and user ports of Port Cards and IN 1 and OUT 1 ports of primary Expansion Cards:
  - Proprietary composite of:
    - IBM PS/2, PC/AT, or Sun compatible keyboard;
    - PS/2, RS-232 serial (except on user ports), or Sun compatible mouse; and
    - Video (see **Standards** above);
  - With the KV99MCON converter, also supports ADB (Mac compatible) keyboard and mouse ports;
  - IN 1 and OUT 1 also carry system-control signals;
- On Expansion Cards' other IN and OUT ports: Proprietary video composite (see **Standards** above);
- On serial ports of Port Cards: EIA/TIA RS-232 proprietarily pinned on RJ-12 ("6-wire RJ-11") connectors, DTE

Resolution: Up to 1280 x 1024, but will depend on the length of CPU and User Cables in your system

Serial (RS-232) Characteristics:
- Protocol: Asynchronous;
- Data format: 8 data bits, 1 stop bit, no parity (fixed);
- Data rate: 9600 or 57,600 bps

Maximum Distance:
- 20 ft. (6.1 m) of CPU or User Cable—possibly as much as 100 ft. (30.5 m) if Cable is coaxial, depending on CPUs, monitor, and video resolution—from any Affinity Port Card to any device attached to it;
- 100 ft. (30.5 m) of Expansion Cable between any two Affinity units;
- 50 ft. (15.2 m) of serial cable from the RS-232 port of any Affinity Port Card to a computer's serial port

User Controls:
- For system: Keyboard commands and on-screen menus;
- On Affinity chassis: Rear-mounted ON/OFF rocker switch(es);
  - KV13xDA models: (2);
  - All other models: (1);
- On all Expansion Cards (KV1305C and KV1306C): Board-mounted BUS/RING jumper;
- On 8-User Expansion Cards (KV1306C): (2) Board-mounted jumper blocks for user-port numbering

Indicators:
- All models: ON/OFF switch(es) are dark when ServSwitch Affinity is OFF, backlit when Affinity is ON;
- KV13xDA models: (3) Front-mounted power-supply status LEDs:
  - (1) for supply 1 (the upper transformer), lit while supply is outputting power;
  - (1) for supply 2 (the lower transformer), lit while supply is outputting power;
  - (1) for the Affinity chassis (marked "SYSTEM"), lit while either supply is outputting power unless internal diodes have failed

Connectors:
- All rear-mounted;
- On Affinity chassis: IEC 320 male power inlet(s):
  - KV13xDA models: (2);
  - All other models: (1);
- On all Affinity Port Cards (KV1300C and KV1301C):
  - (4) DB25 female for CPU connections,
  - (1) RJ-12 ("6-wire RJ-11") female for serial management;
- On 1 x 4 Port Cards (KV1301C):
  - (1) DB25 female for user connections;
- On 4-User Expansion Cards (KV1305C):
  - (2) DB15 female: (1) for input to Port Cards in slots 1 and 2, (1) for input to Port Cards in slots 3 and 4;
  - (2) DB15 male: (1) for output from Port Cards in slots 1 and 2, (1) for output from Port Cards in slots 3 and 4
- On 8-User Expansion Cards (KV1306C):
  - (4) HD15 female:
    - (1) for input to Port Cards set as KVM 1/2 or 9/10;
    - (1) for input to Port Cards set as KVM 3/4 or 11/12;
    - (1) for input to Port Cards set as KVM 5/6 or 13/14;
    - (1) for input to Port Cards set as KVM 7/8 or 15/16;
  - (4) HD15 male:
    - (1) for output from Port Cards set as KVM 1/2 or 9/10;
    - (1) for output from Port Cards set as KVM 3/4 or 11/12;
    - (1) for output from Port Cards set as KVM 5/6 or 13/14;
    - (1) for output from Port Cards set as KVM 7/8 or 15/16

Maximum Altitude:
10,000 ft. (3048 m)

Temperature Tolerance:
32 to 113°F (0 to 45°C)

Humidity Tolerance:
5 to 80% noncondensing

Enclosure: Steel

Fuses: KV13xDA models: Autoresetting switch fuses that cut in when power surges exceed the maximum ratings of the chassis

Power:
- Input: 90 to 264 VAC, 47 to 63 Hz, 700 mA from AC outlet(s) through included power cord(s) and inlet(s) into internal transformer(s):
  - KV13xDA models: Dual transformers with separate AC inlets, electrically isolated from one another;
  - All other models: Single transformer;
- Consumption: Up to 40 VA (40 watts)

Size:
- KV139A and KV139DA chassis: 7"H (4U) x 16.7"W x 7"D (17.8 x 42.4 x 17.8 cm);
- All other Affinity chassis: 5.25"H (3U) x 16.7"W x 7"D (13.3 x 42.4 x 17.8 cm);
- Port Cards and Expansion Cards: 0.9"H x 13.9"W x 4.8"D (2.3 x 35.3 x 12.2 cm);
- Terminator Card (4-User models only): 0.4"H x 2.1"W x 0.8"D (1 x 5.3 x 2 cm)

Weight:
- KV130A, KV130DA, KV138A, and KV138DA: 10.5 lb. (4.8 kg);
- KV132A: 12 lb. (5.5 kg);
- KV134A: 14 lb. (6.4 kg);
- KV139A and KV139DA: 11 lb. (5 kg);
- KV1300C, KV1301C, and KV1306C: 0.9 lb. (0.4 kg);
- KV1304C: 0.2 lb. (0.1 kg);
- KV1305C: 0.4 lb. (0.2 kg)

Ordering Information (continued)

ITEM	CODE

NOTE: For CPU and User Cables, specify length by adding any of these suffixes to the product code (not all cables are available in all lengths):
"-0001" for 1 ft. (0.3 m, User Cables only),
"-0005" for 5 ft. (1.5 m),
"-0010" for 10 ft. (3 m),
"-0020" for 20 ft. (6.1 m),
"-0035" for 35 ft. (10.7 m),
"-0050" for 50 ft. (15.2 m),
"-0075" for 75 ft. (22.8 m), or
"-0100" for 100 ft. (30.5 m)

*You will need a **CPU Cable** for each CPU you attach:*

Standard CPU Cables, available in standard lengths up to 20 ft. (6.1 m)—Mac styles require keyboard/mouse conversion

IBM PS/2 style	EHN051
IBM PC/AT style	EHN048
Mac style with legacy DB15 video connectors	EHN215
Mac style with HD15 VGA video connectors for G3™, G4™, and similar models	EHN550

Coaxial CPU Cables—IBM and Sun styles available in all standard lengths, SGI and RS/6000 styles available in standard lengths up to 20 ft. (6.1 m), Mac styles require keyboard/mouse conversion

Universal IBM style	EHN282
Sun style with traditional 13W3 video connectors	EHN206
Sun style with VGA (HD15) video connectors	EHN515
SGI style	EHN500
RS/6000 style	EHN520
Mac style with traditional DB15 video connectors	EHN208
Mac style with HD15 VGA video connectors for G3, G4, and similar models	EHN560

ServSwitch™ Micro Mac® Converter to convert PS/2 kbd/mouse to ADB™ kbd/mouse signals	KV99MCON
For older Mac models that must see monitor ID: Mac® Video Adapter for ServSwitch™	KV99MA

*You will need a **User Cable** for each monitor/keyboard/mouse user station you attach:*

Regular (non-coaxial) User Cables, available in standard lengths up to 20 ft. (6.1 m)

IBM PS/2* style	EHN054
Sun style with VGA (HD15) video connector for multisync monitor	EHN059

Coaxial User Cables

IBM PS/2* style, available in all standard lengths except 1 ft. (0.3 m)	EHN283
Sun style with 13W3 video connector for Sun monitor, available in all standard lengths	EHN201
Sun style with VGA (HD15) video connector for multisync monitor, available in all standard lengths	EHN225
SGI style, 1 ft. (0.3 m) only	EHN501-0001
RS/6000 style, 1 ft. (0.3 m) only	EHN521-0001

*We no longer offer IBM PC/AT type User Cables for the ServSwitch Affinity, because its current firmware does not support serial mice, although it will still translate signals from PS/2 type mice into serial protocol for PC/AT CPUs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 831
Doc. 3698

Ordering Information (continued)

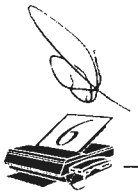
ITEM	CODE
You might also need:	
Expansion Cables for 4-User Units	
10 ft. (3 m)	KV140010
20 ft. (6.1 m)	KV140020
35 ft. (10.7 m)	KV140035
50 ft. (15.2 m)	KV140050
100 ft. (30.5 m)	KV140100
Expansion Cables for 8- and 16-User Units	
10 ft. (3 m)	KV180010
20 ft. (6.1 m)	KV180020
35 ft. (10.7 m)	KV180035
50 ft. (15.2 m)	KV180050
100 ft. (30.5 m)	KV180100
Replacement 6-wire straight-through-pinned flat-satin cable for serial management (specify length)	EL06MS-MM
Rackmount Kits	
To mount 4- or 8-User units in 19" Racks	RMK19A
To mount 4- or 8-User units in 23" Racks	RMK23A
To mount 4- or 8-User units in 24" Racks	RMK24A
To mount 16-User units in 19" Racks	RMK19A139
To mount 16-User units in 23" Racks	RMK23A139
To mount 16-User units in 24" Racks	RMK24A139
Surge protector for IBM PS/2 style keyboard and mouse lines (6-pin mini-DIN M/F)	SP519A-R2
Surge protector for IBM PC/AT style keyboard lines (5-pin DIN M/F)	SP518A-R2

Call Black Box Tech Support for help determining your best options for AC-power backup and protection.

Black Box offers the best warranty program in the industry—Fido Protection*. For more information, request **FaxBack 22512**.

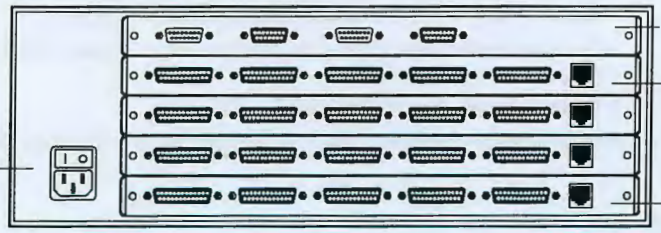
BLACK BOX, the ◆ logo, and Fido Protection are registered trademarks, and ServSwitch and ServSwitch Affinity are trademarks, of Black Box Corporation.

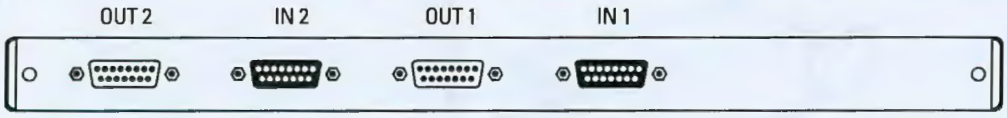
All other trademarks mentioned in this document are acknowledged to be the property of the trademark owners.



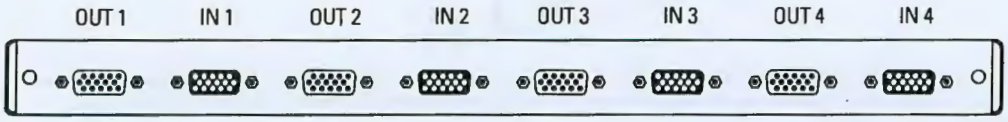
If you need to share access to a large number of CPUs, think about putting in an Affinity daisychain made up of 4-User Expansion Chassis (like the fully loaded one shown below) or 8- or 16-User Chassis. They come empty (no Cards installed), but you can install one Expansion Card (or two in the 16-User units) and add as many as four 0 x 4 or 1 x 4 Port Cards to them, giving you a maximum of four, eight, or sixteen user stations and sixteen CPUs attached to each unit. (Keep in mind that however many user stations a unit is designed for, only that many video paths can be open through that unit at a time. For example, a 4-User unit only has four video paths, so if there are already four users attached to a 4-User unit, and a user at another Affinity unit selects one of the 4-User unit's CPUs, one of the 4-User unit's users—and all other users on that slot—will be locked out until the new connection ends.)

The 8-User units look very similar to the 4-User unit shown here, but they accept only 8-User Expansion Cards like the one shown below. The 16-User Units accept two of the 8-User Expansion Cards. The 8-User Cards have jumper blocks that you can set to control which four KVM slots are used by the users attached to the Affinity chassis that the Card is installed in: KVM 1 through 4, 5 through 8, 9 through 12, or 13 through 16.





DB15 female expansion ports on 4-User Expansion Card (KV1305C)



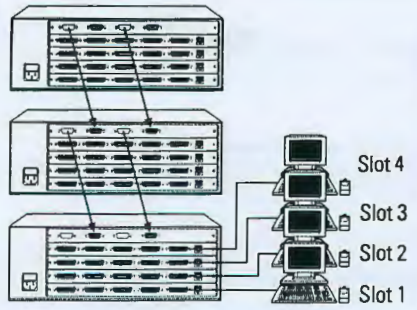
HD15 female expansion ports on 8- and 16-User Expansion Card (KV1306C)

On the 4-User Expansion Cards (above, top), IN 1 and OUT 1 carry signals for the Port Cards in slots 1 and 2, while IN 2 and OUT 2 carry signals for the Port Cards in slots 3 and 4.

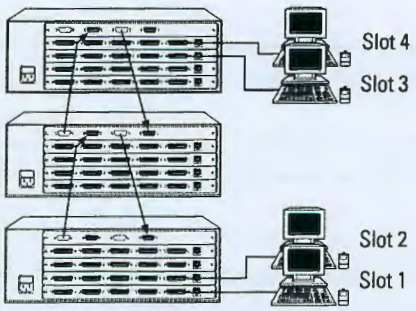
On the 8-User Expansion Cards (above, bottom), IN 1 and OUT 1 carry the signals for either KVM 1 and 2 or, if installed in the bottom slot of a 16-User unit, KVM 9 and 10; IN 2 and OUT 2 cary the signals for either KVM 3 and 4 or KVM 11 and 12; and so on. A pair of jumper blocks, mentioned above, determines which four KVM slots the four users on that Affinity chassis will use.

Because the control paths are carried on different connectors this way, you have maximum flexibility for designing your daisychain layout:

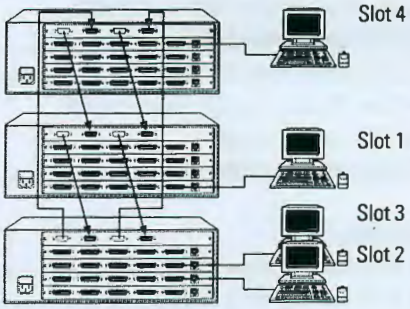
- If all of your users are on one Chassis, use the regular bus topology (below, left).
- If you have two users on one Chassis and two on another, use the "split bus" topology (below, middle).
- If your users are spread across several Chassis, use the ring topology (below, right).*



Regular Bus



Split Bus



Ring

*It is always important to keep in mind that only one user at a time can use the bus that interconnects daisychained Affinity units, especially when you implement a ring topology. For example, when your Affinity units are interconnected in a ring, if any user on Slot 1 selects a CPU attached to an Affinity unit other than his own, no other Slot 1 user can select any CPUs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 835
Doc. 3698

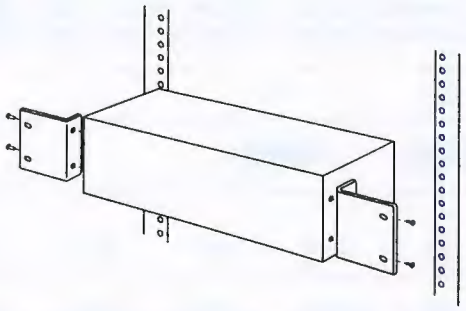
The complete package

- The ServSwitch Affinity, including any cards and blanking plates that are normally preinstalled with your model. (Blanking plates will cover all unused slots, as well as the slot on 4-User models that the tiny Terminator Card is installed in.)
- A power cord.
- *KV13xDA models only:* A second power cord.
- A 6-ft. (1.8-m) serial cable with RJ-12 ("6-wire RJ-11") plugs.
- An RJ-12 to DB9 modular adapter.
- A manual.

What else you might need

- CPU Adapter Cables, User Adapter Cables, and (if you're cascading) Expansion Cables.
- Keyboards, mice, and monitors for your users. If you're mixing platforms, we recommend true multiscan, multisync monitors capable of syncing to each CPU's video-output frequencies and compatible with all of the CPUs' video cards. Also, if one of the multiple platforms is IBM, the monitors must be able to accept both separate H/V sync and composite sync. (Such monitors are widely available.) We recommend that the monitors be able to display a maximum resolution of not less than 1280 x 1024 at a maximum refresh rate of not less than 75 Hz.
- An AC-power surge protector and uninterruptible power supply.
- Data-line surge protectors for the keyboard and mouse lines.
- *To attach an Apple Mac®:* A ServSwitch™ Micro Mac® Converter (product code KV99MCON), a G3™/G4™ or legacy Macintosh® style CPU-Extension Cable, and, if the Mac needs to see ID bits from its monitor, a Mac Video Adapter for ServSwitch (KV99MA).
- *If you purchase a 4-User Expansion Chassis or an 8- or 16-User Chassis:* Port Cards for your CPU and user-station connections.
- *To cascade a ServSwitch Affinity:* An Expansion Card.
- *To rackmount a ServSwitch Affinity:* A ServSwitch Affinity Rackmount Kit.

If you can use a screwdriver, you can install the Rackmount Kits.



Ordering Information

ITEM	CODE
ServSwitch Affinity	
4-User Expansion Chassis (Terminator Card installed, no Port Cards installed)	
Single power supply	KV130A
Dual power supply	KV130DA
4-User Standalone Chassis	
2 Users by 8 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 and 2)	KV132A
4 Users by 16 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 through 4)	KV134A
8-User Chassis (no Cards installed)	
Single power supply	KV138A
Dual power supply	KV138DA
16-User Chassis (no Cards installed)	
Single power supply	KV139A
Dual power supply	KV139DA
Port Cards	
0 x 4 (No Users, Four CPUs)	KV1300C
1 x 4 (One User, Four CPUs)	KV1301C
4-User Terminator Card	KV1304C
4-User Expansion Card	KV1305C
8- and 16-User Expansion Card	KV1306C

Apêndice IQ

RQS nº 03/2005 - CN
CPMI - CORREIOS
0830
Fls. Nº
3698
Doc.

Layer 2 switching

A switch helps provide a clear path from each workstation to its destination on demand, whether that destination is another workstation or a server. In contrast with bridges and routers (which process data packets on an individual, first-come, first-served basis), switches maintain multiple, simultaneous data conversions among attached LAN segments.

From an end-user workstation's perspective, a switched circuit appears as a dedicated connection—a direct, full-speed LAN link to an attached server or other remote LAN node. Although this technique is somewhat different from what a LAN bridge or router does, switching hubs are based on similar technologies.

Switching hubs that use bridging technologies are called Layer 2 switches—a reference to Layer 2 or the Data Link Layer of the OSI Model. These switches operate using the MAC addresses in Layer 2 and are transparent to network protocols. Layer 2 switches connect different parts of the same network, as determined by the network number contained with the data packet.

If you're subdividing an existing LAN, obviously you're dealing with only one network and one network number, so you can install a Layer 2 switch wherever it will segment network traffic the best, and you don't have to reconfigure the LAN.

If, on the other hand, you use a Layer 3 switch, which uses network addresses, you'd have to reconfigure the segments to ensure that each has a different network number.

Similarly, if you're connecting existing networks, you have to examine the currently configured network numbers before adding a switch. If the network numbers are the same, you need to use a Layer 2 switch. If they're different, you must use a Layer 3 switch.

When dealing with multiple existing networks, you'll find they usually use different network numbers. In this case, it's preferable to use a Layer 3 switch (or possibly even a full-featured router) to avoid reconfiguring the network.

Layer 2 switches are generally unmanaged and are recommended for smaller, less-complex networks.

Store-and-forward switches

Store-and-forward networking switches read each complete data packet into an internal buffer, temporarily storing the packet. The destination and source addresses are checked against the switch's internal address list—just like a bridge. Simultaneously, the entire packet undergoes an error-checking procedure to validate its integrity. This process requires that the whole packet be read, since the check digit is the very last character in the packet. Once verified, the packet is forwarded from the buffer to the appropriate destination device.

Black Box offers the best warranty program in the industry—Fido Protection®. For more information, request **FaxBack 22512**.

Ordering Information

ITEM	CODE
Express Ethernet Switches	
10-/100-Mbps Copper	
(8) RJ-45	LB9108A
(16) RJ-45	LB9019A
(24) RJ-45	LB9020A
10-/100-Mbps Copper, 100-Mbps Fiber	
(1) RJ-45, (1) SC	LB9002A-SC-R2
(1) RJ-45, (1) ST	LB9002A-ST-R2
(2) RJ-45, (6) SC	LB9006A-SC
(2) RJ-45, (6) ST	LB9006A-ST
(6) RJ-45, (2) SC	LB9021A
(6) RJ-45, (2) ST	LB9022A
(7) RJ-45, (1) SC	LB9007A-SC-R2
(7) RJ-45, (1) ST	LB9007A-ST-R2
100-Mbps Fiber	
(8) SC	LB9008A-FO
10-/100-Mbps Copper, 100-Mbps Fiber, Modular	
(16) RJ-45,	
(1) Slot for Optional Fiber Uplink	LB9017A-R2
(24) RJ-45,	
(1) Slot for Optional Fiber Uplink	LB9024A
Choose an uplink module for LB9017A-R2 and LB9024A	
100BASE-FX SC Module	LB9017C-SC
100BASE-FX ST Module	LB9007C-ST

NOTE: *The LB9006A–LB9007A models, LB9008A-FO, LB9017A-R2, LB9019A–LB9022A, and LB9024A ship with* [redacted]

For optimum performance and a 20% savings, order...

Category 5 Patch Cable, 100-MHz, 4-Pair, Straight-Pinned, PVC, Beige	EVMSL05
Duplex Fiber Optic Cable, PVC	
ST-ST	EFN062
SC-SC	EFN4025

RQS nº 03/2005 - CN
CPMI - CORREIOS
837
Fls. Nº
Doc. 3698

a network into 10-/100-Mbps copper segments and 100-Mbps fiber segments.

Choose from ST® or SC connectors on the 100BASE-FX side. Each switch has a push-button uplink for linking to another device. Use these switches at the desktop or in racks. Rackmount hardware is included.

The 2-port switches are ideal for adding a 100-Mbps fiber island to your existing network or for extending a network long distances over fiber optic cable. To handle the heavy traffic load associated with this sort of network link, the 2-port switches support a whopping 8192 MAC address entries!

The 8-port switches are good switches for integrating 100-Mbps fiber into your existing 10-/100-Mbps network. The extra distance from fiber means you can extend network segments up to 1.2 miles (2 km).

The LB9006A-SC, LB9006A-ST, LB9021A, and LB9022A models provide DIP switches for controlling port operation manually.

For greater versatility, the LB9007A-R2 models have a console port that enables you to control ports and set up port-based VLANs and trunking. The 8-port switches support 1024 MAC address entries.

Both LB9007A-R2 models support managment. The managament type is an ASCII console port (cable included) that provides access to a text-based menu. The menu permits basic configuration of port parameters (such as changing speed or duplex settings), and has a proprietary method for assigning the ports into VLAN and Port-Trunking groups.

100-Mbps Fiber (LB9008A-FO)

For simplicity, speed, and distance, choose this fiber-only switch. It provides eight ports of blazing speed and distances of up to 1.2 miles (2 km) with all the security of fiber. Best of all, this entry-level switch is super simple to set up—just plug-and-play.

The switch has SC-style fiber connectors and supports 1024 MAC address entries. It has DIP switches and is easy to rackmount with the included hardware.

10-/100-Mbps Copper, 100-Mbps Fiber, Modular (LB9017A-R2, LB9024A) and Optional Fiber Uplink Modules (LB9017C-SC, LB9017C-ST)

These Express Ethernet Switches feature 16 or 24 autosensing 10-/100-Mbps RJ-45 ports. They're a smart-priced way to quickly expand your 10BASE-T/100BASE-TX network with the option of adding a fiber uplink later if you need it.

Although the switches are easy to set up, they offer powerful features to help you control heavy network loads. The 2048 MAC address table handles a large number of end users.

These modular switches also include an RS-232 console port for basic management (cable included). Through the console port, you can access proprietary port-based VLAN features that enable you to segment or isolate traffic at Layer 2.

Trunking provides extra bandwidth of up to 400 Mbps between two connected switches. You can also regulate standard backpressure and auto-negotiation on individual ports. The crossover button enables you to configure one port as an uplink. These switches occupy only 1U of rack space and are easily rackmountable with the included hardware.

Both LB917A-R2 and LB9024A support managment. The managament type is an ASCII console port (cable included) that provides access to a text-based menu. The menu permits basic configuration of port parameters (such as changing speed or duplex settings), and has a proprietary method for assigning the ports into VLAN and Port-Trunking groups.

Specifications

Distance (Maximum):
RJ-45 ports: 100 m (328 ft.);
Fiber ports: 2 km (1.2 mi.)

Forwarding Rate:
14,880 pps at 10 Mbps;
148,800 pps at 100 Mbps

MAC Addresses: LB9108A, LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2, LB9008A-FO: 1024;
LB9002A-SC-R2, LB9002A-ST-R2: 8192;
LB9019A–LB9020A, LB9017A-R2, LB9024A: 2048

Standards: IEEE 802.3 (10BASE-T), IEEE 802.3u (100BASE-TX/FX)

Switching Method: Store-and-forward

VLAN Support: LB9007A-SC-R2, LB9007A-ST-R2, LB9017A-R2, LB9024A: Proprietary port-based

Indicators:
LB9108A:
Per-unit LEDs: (1) Power;
Per-port LEDs:
(1) 100 Mbps/TX,
(1) 10 Mbps/RX,
(1) Full-Duplex/Collision;
LB9019A–LB9020A:
Per-unit LEDs: (1) Power;
Per-TX port LEDs:
(1) Link/Activity, (1) 10-/100-Mbps Speed, (1) Duplex/Collision, (1) 100 Mbps/TX, (1) 10 Mbps/RX, (1) Full-Duplex/Collision;
LB9002A-SC-R2, LB9002A-ST-R2:
Per-unit LEDs: (1) Power;
Per-port LEDs:
(1) Link, (1) 100 Mbps, (1) TX/RX, (1) Duplex/Collision, (4) Utilization;
LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2:
Per-unit LEDs: (1) Power, (1) Uplink;
Per-TX port LEDs:
(1) 10-/100-Mbps Speed, (1) Link, (1) TX, (1) Collision, (1) RX, (1) Duplex, (4) Utilization;
Per-FX port LEDs: (1) Link, (1) Activity, (1) Full-Duplex;
LB9017A-R2, LB9024A:
Per-unit LEDs: (1) Power, (1) Uplink, (1) Module Enable;
Per-TX port LEDs:
(1) 100 Mbps/TX,
(1) 10 Mbps/RX,
(1) Full-Duplex/Collision;
LB9008A-FO:
Per-unit LEDs: (1) Power, (1) Uplink;
Per-FX port LEDs: (1) Link, (1) Activity, (1) Full-Duplex

Temperature:
Operating: 32 to 104°F (0 to 40°C);
Storage: -13 to +158°F (-25 to +70°C)

Humidity: 10 to 90% noncondensing

Power: 100–240 VAC, 50–60 Hz, autosensing, internal

Size:
LB9108A, LB9002A-SC-R2, LB9002A-ST-R2: 1.4"H x 10"W x 5.3"D (3.6 x 25.4 x 13.5 cm);
LB9019A, LB9021A–LB9022A: 1.75"H x 10.2"W x 8"D (4.4 x 25.9 x 20.3 cm);
LB9020A, LB9006A-SC, LB9006-ST, LB9007A-SC-R2, LB9007A-ST-R2, LB9017A-R2, LB9024A, LB9008A-FO: 1.75"H x 17.3"W x 8"D (4.4 x 43.9 x 20.3 cm)

Weight: LB9108A: 3.5 lb. (1.6 kg);
LB9019A–LB9020A, LB9017A-R2, LB9024A: 5.7 lb. (2.6 kg);
LB9002A-SC-R2, LB9002A-ST-R2: 2.1 lb. (1 kg);
LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2: 5.5 lb. (2.5 kg);
LB9008A-FO: 6.5 lb. (2.9 kg)

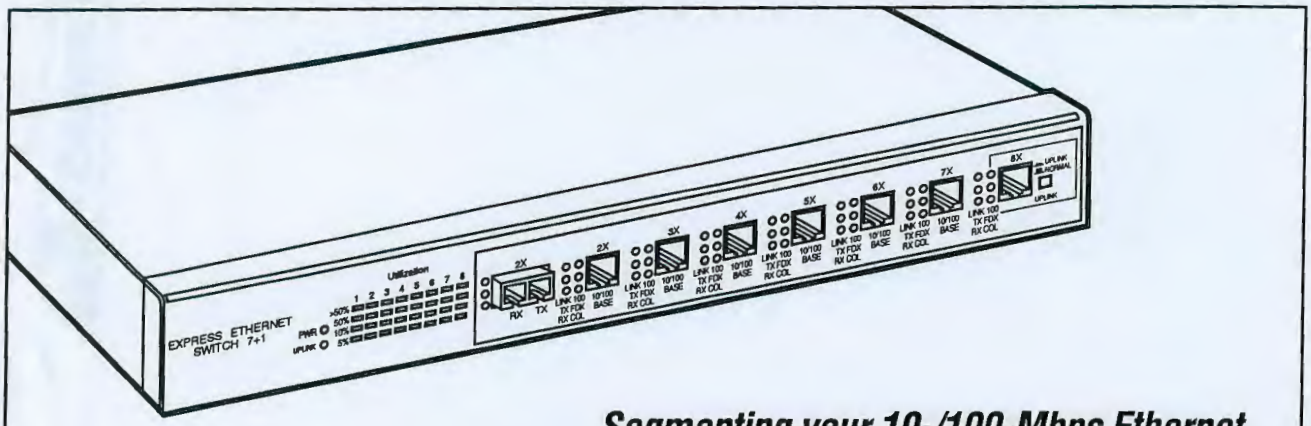
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 838
Doc. 3698

© 2003. All rights reserved.
Black Box Corporation.

BLACK BOX® NETWORK SERVICES

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

EXPRESS ETHERNET SWITCHES



Segmenting your 10-/100-Mbps Ethernet LAN doesn't have to be expensive!

Key Features

- ***Low-cost switching for small- or mid-sized networks.***
- ***Protocol-independent, MAC-layer switching.***
- ***Models for copper, fiber, copper and fiber, or copper with a fiber uplink.***
- ***Fiber ports provide extra distance of over a mile.***
- ***Half-/full-duplex on all RJ-45 ports.***
- ***Reduce bottlenecks.***
- ***Include universal power supply.***

High-speed switching technology at an affordable cost—get the best of both worlds with BLACK BOX® Express Ethernet Switches.

These well-engineered machines provide you with dedicated high-speed workgroups, plus they improve network performance and keep data moving freely and quickly.

Express Ethernet Switches enable you to put a full wire-speed switch right into a network without making a large investment. Plus they're available in a wide variety of port options, from a 2-port model for small network extension to a 24-port switch with optional fiber uplink for mid-sized networks.

And if you want options, these switches have them! Each switch provides true Layer 2 nonblocking switch architecture and a store-and-forward switching engine. With Layer 2 switching, you get the speed to handle lots of network data. The store-and-forward engine checks the integrity of each data packet and ensures accurate throughput.

All Express Ethernet Switches have an autosensing power supply that adapts to worldwide voltages, so they integrate quickly and easily with your existing equipment. A crossover switch makes uplinking to other switches or hubs easy. Extensive LEDs provide port status.

All RJ-45 ports operate at 10/100 Mbps in half- or full-duplex mode. The fiber ports are for 100-Mbps connections in either half-or full-duplex mode.

10-/100-Mbps Copper (LB9108A, LB9019A–LB9020A)

These switches feature 8, 16, or 24 autosensing 10-/100-Mbps RJ-45 ports. They're perfect for rapid, inexpensive network expansion or building workgroups. Because the autosensing ports adjust to the speed and duplexity of each port automatically, setup is a breeze.

The 8-port model supports 1024 MAC address entries and is great for building small workgroups. It's housed in a compact, sturdy enclosure suitable for desktop use or wallmounting.

For higher traffic loads and larger networks, the 16- and 24-port switches support 2048 MAC addresses. A crossover button enables you to configure one port as an uplink. The 16- and 24-port switches include a rackmount kit.

10-/100-Mbps Copper, 100-Mbps Fiber (LB9002A-SC-R2, LB9002A-ST-R2, LB9006A-SC, LB9006A-ST, LB9021A–LB9022A, LB9007A-SC-R2, LB9007A-ST-R2)

Available in sporty 2-port models or in more robust 8-port versions, these switches divide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 839
Doc 3698

Doc.
000233

CPL/AC

PREGÃO 050/2003

LOCAÇÃO DE EQUIPAMENTO DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

ITAUTEC INFORMÁTICA S/A

PROPOSTA ECONÔMICA

2003
PASTA 15

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 840
Doc. 3698

Itautec

Brasília, 24 de julho de 2003. CT/FGCO/279/2003

A
Empresa Brasileira de Correios e Telégrafos – ECT
Comissão Permanente de Licitação da Administração Central - CPL/AC
SBN – Quadra 01 – Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília - DF

Ref.: Pregão 050/2003 – CPL/AC
Data: 24/07/2003 às 9:00 Horas

Prezados Senhores,

De acordo com a solicitação contida no referido convite, estamos encaminhando, em anexo, nossa Proposta nº 128/2003, a fim de participarmos do processo de licitação, do Pregão 050/2003 – CPL/AC, para Locação de equipamentos de informática, incluindo a assistência técnica e treinamento de pessoal, conforme especificação técnica descrita em nossa proposta.

Por oportuno, comunicamos os dados de nossa Empresa, participante deste processo licitatório:

- Unidade Licitante
- Razão Social: ITAUTEC INFORMÁTICA S.A. - GRUPO ITAUTEC PHILCO
- Endereço: Rua Santa Catarina nº 01 – Tatuapé - CEP 03086-025
- Município/UF: São Paulo - SP
- CNPJ Nº/IE Nº: 51.764.058/0001-42 / 110.970.918.117
- Banco/Agência: Banco do Brasil S.A. - Agência nº 3064-3 - C/C nº 7999-5

- Dados para contato - Filial Brasília - DF
- Contato: Jorge Ítalo Dimatteu Telles
- CPF 292.880.961-91
- Endereço: SCS Q. 01 - Bloco "F" Ed. Camargo Corrêa 11º Andar - CEP 70397-900
- Município/UF: Brasília-DF
- Telefone: (61) 323-3031 Ramal: 1126 - (61) 9994-4021
- Fac-símile: (61) 226-1251
- E-mail: italo@itautec.com.br

Sem mais, colocamo-nos à disposição de V.Sas. para outras informações complementares que se façam necessárias.

Cordialmente,

Itautec Informática S.A
Grupo Itautec Philco
Jorge Ítalo Dimatteu Telles
Representante de Marketing

Itautec Informática S.A.
Grupo Itautec Philco
Raimundo Carlos Pereira
Gerente Comercial

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 841
Doc.

Itautec

1005

A
Empresa Brasileira de Correios e Telégrafos – ECT
Comissão Permanente de Licitação da Administração Central - CPL/AC
SBN – Quadra 01 – Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília - DF

PROPOSTA ECONÔMICA

Pregão 050/2003 – CPL/AC

Itautec

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls - Nº 842
Doc. 3698

Itautec

Dados de Cadastro

ITAUTEC INFORMÁTICA S.A. - GRUPO ITAUTEC PHILCO
CNPJ Nº: 51.764.058/0001-42
Inscrição Estadual: 110.970.918.117
Rua Santa Catarina nº 01 – Tatuapé - CEP 03086-025
Telefones: (61) 323-3031 Ramal: 1126 - (61) 9994-4021
Fax: (61) 226-1251
E-mail: italo@itautec.com.br

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 843
Doc. 3690

Itautec

ÍNDICE

1. Requisitos Gerais 5
2. Descrição dos Serviços 22
   2.1 Instalação de Infra Elétrica para a Sala Cofre 22
   2.2 Implementação de Servswitch 28
   2.3 Implementação da Conectividade da Rede 32
   2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager 38
   2.5 Serviço de Implementação de Ambiente pSeries Regatta, Storage e Backup 48
   2.5.1 Ilustração da Solução 59
   2.6 Implementação do IBM Director 61
   2.7 Implementação do gerenciamento eHealth Enhanced Sysedge 63
   2.8 Treinamento Oficial 66
3. Pauta de Distribuição e Especificações Técnicas dos Equipamentos. 72
   3.1 Pauta de Distribuição 72
4. Configuração de Equipamentos 207
   4.1 Brasília 207
   4.2 São Paulo 218
5. Aspectos Financeiros 233

ANEXO 1 – ATESTADOS DE VISTORIA

ANEXO 2 – DECLARAÇÕES E CERTIFICAÇÕES

ANEXO 3 – CATÁLOGOS, MANUAIS E OUTROS DOCUMENTOS TÉCNICOS

ANEXO 4 – OUTROS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0841
Doc. 3698

Itautec

1. Requisitos Gerais

1.1. ASPECTOS GERAIS

- Cabe à ITAUTEC fornecer, garantir compatibilidade e portabilidade, conforme Item 1.6, instalar, configurar, dar garantia e assistência técnica aos produtos fornecidos e treinar a equipe técnica da ECT, durante a vigência do contrato;
- O fornecimento contemplará os produtos descritos nesta Proposta, provendo a:
  - ✓ Preparação do ambiente de produção, realizando integração e interoperabilidade com o ambiente já existente (Rede TCP/IP e Segurança de Rede);
  - ✓ Integração e interoperabilidade da Rede SAN – Storage Area Network, existente na Empresa Brasileira de Correios e Telégrafos à Rede SAN fornecida, de forma que os Servidores e o Sistema de Backup fornecidos pela ITAUTEC possam acessar os dados armazenados no atual sistema de armazenamento (Storage IBM 2105 F20), com a performance compatível com as aplicações existentes.
- Os produtos descritos nesta Proposta possuem quantidades e especificações mínimas para a execução das funcionalidades solicitadas. produtos adicionais, necessários ao cumprimento das exigências funcionais e de performance, verificadas durante a vigência do Contrato, serão fornecidos pela ITAUTEC;
- Cabe à ITAUTEC, a obrigatoriedade de fornecer, instalar e configurar, a critério exclusivo da ECT, as atualizações e correções de todos os softwares fornecidos,englobando, inclusive, a evolução das versões, sem ônus adicionais à ECT, durante a vigência do Contrato;
- Será de exclusiva responsabilidade da ITAUTEC a entrega, a instalação, a configuração, os testes, a garantia e assistência técnica dos produtos, bem como o fornecimento dos recursos adicionais que sejam necessários ao pleno atendimento das funcionalidades exigidas no Edital;
- A ITAUTEC procederá à entrega e a instalação física de todos os produtos nas Salas de Segurança Física, nas cidades de Brasília/DF e São Paulo/SP, conforme Pauta de Distribuição e Especificações Técnicas dos Equipamentos;
- Serão fornecidos pela ITAUTEC, quando da instalação dos produtos, os insumos, suprimentos e componentes, tais como: cabos, acessórios, mídias, manuais e documentações necessárias;
- Serão fornecidos pela ITAUTEC todos os controladores (drivers) necessários para o funcionamento dos equipamentos fornecidos, bem como todos os demais programas necessários à instalação, configuração e diagnóstico dos equipamentos, periféricos e interfaces;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Doc. 3698

- A ITAUTEC, na data de assinatura do contrato, apresentará equipe de trabalho e seus integrantes, relacionando-os nominalmente e informando currículo e telefone para contato, devendo ser alocado um profissional como gestor do projeto durante a vigência do Contrato;
- O gestor do projeto alocado é certificado em PMP (Project Management Professional) pelo PMI (Project Management Institute) e cópia desta certificação, atualizado e vigente, consta na Proposta Econômica da ITAUTEC;
- A ECT poderá solicitar, a qualquer momento da vigência do Contrato, a seu critério, a substituição de qualquer membro da equipe de trabalho, comprometendo-se a comunicar com antecedência de 15 (quinze) dias;
- A ECT indicará, na data da assinatura do contrato, o nome do Gestor e o nome dos componentes da sua equipe técnica para coordenar e orientar todo o processo de instalação, configuração e testes dos produtos, cabendo ao Gestor acompanhar o cumprimento dos prazos e atestar a qualidade dos produtos entregues;
- A ITAUTEC detalhará o plano de trabalho, conforme Item 1.2 desta Proposta, para implantação dos produtos, informando o cronograma de atividades detalhado em fases, atividades, prazos e recursos alocados;
- Caso a ITAUTEC não seja a fabricante de algum dos produtos fornecidos, mas apenas distribuidora da mesma, esta apresentará CARTA DE SOLIDARIEDADE do fabricante, assegurando o fornecimento e a garantia do produto em questão. Entretanto, se a mesma for apenas fornecedora do produto, esta pode apresentar CARTA DE SOLIDARIEDADE do fabricante ou CARTA DE SOLIDARIEDADE do distribuidor, sendo que neste caso também deve ser entregue CARTA DE SOLIDARIEDADE do fabricante para o distribuidor apresentado;
- No que se refere a produtos, periféricos, acessórios, instalação, garantia, recursos humanos, translado, transporte, hospedagem, embalagens, e outras despesas, diretas e indiretas, necessárias ao cumprimento das obrigações da ITAUTEC, serão de responsabilidade da ITAUTEC e não gerarão qualquer ônus à ECT;
- A ECT poderá, a seu critério, solicitar o deslocamento e/ou movimentação dos equipamentos dentro das Salas de Segurança Física de Brasília-DF e São Paulo-SP. Todos as despesas relativas a esta movimentação serão de responsabilidade da ITAUTEC. A ECT solicitará os deslocamentos durante a vigência do contrato.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

1.2. DETALHAMENTO DO CRONOGRAMA DE TRABALHO

- A ITAUTEC apresentará, para validação da ECT, até 45 (quarenta e cinco) dias após a assinatura do Contrato, cronograma detalhado de atividades contendo, no mínimo, os seguintes itens:

1. Planejamento da adequação dos recursos de suporte à instalação dos equipamentos;
2. Cronograma de Entrega e Instalação dos Equipamentos;
3. Arquitetura detalhada da interligação de todos os produtos fornecidos;
4. Cronograma de Instalação e Configuração do Ambiente Operacional e dos Softwares;
5. Arquitetura planejada para a interconexão dos elementos que compõem a Rede TCP/IP, Rede SAN e a Rede de Segurança com os atuais equipamentos existentes nos CCDs;
6. Planejamento do treinamento dos técnicos da Empresa Brasileira de Correios e Telégrafos .

- Sempre que houver alteração/atualização do cronograma, uma nova versão será imediatamente encaminhada, para validação da ECT, com respectivos relatórios de impacto;
- Qualquer alteração no corpo técnico ou gerencial da ITAUTEC não afetará o cronograma nem tampouco a qualidade dos produtos contratados.

1.2.1. CRONOGRAMA DE EXECUÇÃO

Será obedecido o seguinte cronograma de execução:

Fase	Descrição	Prazo (dias)
I	Apresentação do Cronograma de Trabalho em até	D + 45
II	Entrega, Instalação e Configuração dos Equipamentos em até	D + 90
III	Aceitação Final dos Equipamentos em até	D + 120
IV	Treinamento Operacional em até	FIII + 30
V	Treinamento Oficial em até	FIII + 720
VI	Treinamento On-Site em até	FIII + 1440

Onde: D = Data de Assinatura do Contrato.

FIII = Data de Emissão do Termo de Aceite da Fase III.

1.2.2. O Termo de Aceitação do Cronograma de Trabalho – FASE I será emitido após concluídas as etapas definidas na Minuta de Contrato de Prestação de Serviços.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 847
3698
Doc.

1.3. ENTREGA E INSTALAÇÃO

1.3.1. RECURSOS DE SUPORTE AOS EQUIPAMENTOS

- A ITAUTEC fornecerá, instalará e adequará todas as conexões lógicas e elétricas necessárias à instalação de todos os equipamentos ofertados para os CCDs de Brasília e São Paulo, levando em consideração a padronização e garantia das Salas de Segurança Física – SSF;
- Todos os aspectos relacionados à adequação das instalações lógicas e elétricas serão levantados durante a Vistoria obrigatória, durante este etapa, a ITAUTEC avaliará os detalhes técnicos necessários ao cumprimento de suas obrigações;
- Todos os produtos utilizados na adequação das instalações lógicas e elétricas permanecerão em caráter definitivo na ECT após o término do Contrato;
- Para efeito de quantitativo de conexões lógicas a serem fornecidas e instaladas pela ITAUTEC, serão consideradas todas as interfaces de rede de todos os equipamentos fornecidos, inclusive os equipamentos adicionais, mais o percentual de 25% sobre esta quantidade;
- Para efeito de quantitativo de conexões elétricas a serem fornecidas e instaladas pela ITAUTEC, serão consideradas todas as entradas de energia elétrica de todos os equipamentos fornecidos, inclusive os equipamentos adicionais, mais o percentual de 20% sobre esta quantidade;
- O fornecimento englobará todos os cabos, fibras óticas, conectores, disjuntores, quadros elétricos, leitos aramados, tomadas e demais equipamentos e componentes necessários à interligação de todos os equipamentos ofertados, tanto lógica quanto eletricamente, levando em consideração a padronização e garantia das Salas de Segurança Física – SSF;
- Todos os cabos, conectores e fibras fornecidos serão certificados por órgãos competentes e possuirão o comprimento suficiente para interligar todos os equipamentos. Será entregue um percentual adicional de 20% (vinte por cento) sobre as quantidades fornecidas de cabos de rede e fibras óticas;
- O cabeamento lógico UTP CAT 6 a ser lançado pela ITAUTEC será certificado para suportar operação a velocidade de 1Gbps;
- O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares necessários à instalação são de inteira responsabilidade da ITAUTEC e não gerará ônus à ECT;
- A falta de peças ou equipamentos não será alegada como motivo de força maior e não eximirá a ITAUTEC das penalidades a que estará sujeita pelo não cumprimento dos prazos estabelecidos;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 848
Doc. 3698

- A ITAUTEC entregará toda a documentação da implantação dos produtos, conforme foram implantados, inclusive, alterando as documentações existentes de maneira a retratar as novas configurações dos ambientes das SSF's após a implantação. Serão entregues 4 (quatro) cópias impressas e 4 (quatro) cópias em CDROM de toda a documentação.

1.3.2. RELATÓRIO DE INSTALAÇÃO (RI)

- Será elaborado em formulário impresso e apresentando, no mínimo os seguintes itens:
  - ✓ a Confirmação de todos os requisitos necessários para o perfeito funcionamento de cada produto, nos locais onde estará instalado, de maneira distinta, com um item para cada caso;

- Confirmação da presença e funcionamento adequado de acessórios, cabos de interface, cabos de alimentação, softwares, manual de instalação, manual de operação, manual de manutenção, discriminando um item para cada caso;
  - ✓ Confirmação do perfeito funcionamento do hardware e do software para os todos os produtos;
  - ✓ A identificação de cada produto (marca, modelo, versão de software, número de série e outras informações pertinentes);
  - ✓ A identificação da instalação, condições das tensões de alimentação e demais informações identificadoras da instalação;
  - ✓ Nome, Matrícula, Data e assinatura do técnico da ITAUTEC que instalou o produto;
  - ✓ Nome, Matrícula, Data e assinatura do representante técnico da ECT.

- A ECT, através de seu representante técnico, deve conferir o completo preenchimento do RI. Todas as informações fornecidas nesse RI serão de responsabilidade única da própria ITAUTEC;
- A ECT, através de seu representante técnico e de posse do RI, acompanhará o técnico da ITAUTEC no teste de aceitação do Período de Funcionamento Experimental – PFE, de cada produto, quando serão verificados todos os itens apresentados no RI;
- Quando aprovado o funcionamento de todos os produtos, tendo como base os itens do RI para cada produto, esses produtos serão considerados instalados e aptos a serem utilizados. Isso será confirmado pelo nome, matrícula, data e assinatura do representante técnico da ECT, no RI;
- Quando não aprovado o funcionamento de qualquer produto, a ITAUTEC anotará no RI as ocorrências e suas origens, tomará todas as providências necessárias para resolvê-las, indicando no RI a condução sobre as ocorrências, pelo representante técnico da ECT, sem gerar ônus à ECT e sem prejudicar o tempo previsto de instalação;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0843
Doc. 3690

- O RI não isenta a ITAUTEC das responsabilidades sobre o pleno funcionamento dos produtos, o qual será estendido ao longo de todo o período de garantia;
- A falta da instalação completa de um ou mais produtos constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de instalação de equipamentos correspondente, enquanto perdurar a instalação incompleta;
- Desde que por escrito e a critério da Empresa Brasileira de Correios e Telégrafos , a instalação dos produtos será :
  - ✓ Alterada em sua seqüência;
  - ✓ Prorrogada por prazo determinado.

1.4. INSTALAÇÃO E HOMOLOGAÇÃO DO AMBIENTE

- Após o fornecimento, instalação e configuração dos produtos fornecidos (conforme requisitos de segurança recomendados pelo fabricante e de acordo com a política de segurança da ECT), será estabelecido pela ECT um PFE – Período de Funcionamento Experimental – para testar o perfeito funcionamento dos produtos, verificar as funcionalidades dos mesmos analisando sua aderência às especificações deste Edital e a sua compatibilidade com a estrutura já existente na ECT;
- Durante o PFE, todos os produtos serão testados quanto à configuração realizada. Serão efetivados testes de acesso através da Rede TCP/IP, Rede SAN, Equipamentos de Segurança Lógica bem como a realização de procedimentos de BACKUP e RESTORE.
  - ✓ O período de avaliação pode estender-se por até 7 (sete) dias consecutivos, não devendo ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos, durante este período;
- Todos os produtos, a critério da ECT , serão submetidos ao PFE, sendo que, somente após este processo, pode ser emitido o Termo de Aceitação da Fase III;
- A ITAUTEC entregará todos os comprovantes que atestem o licenciamento dos softwares fornecidos. A relação detalhadas dos softwares e seu quantitativo constarão em planilha a ser entregue à ECT, sendo que, somente após a entrega destes documentos, será emitido o Termo de Aceitação da Fase III;
- Caso ocorra qualquer falha no produto testado, a contagem de tempo será reiniciada a um novo período de tempo. Serão toleradas, no máximo, 3 (três) tentativas. Esgotadas as três tentativas, o processo será suspenso por uma semana e uma última oportunidade de cumprimento de PFE será concedida à ITAUTEC, cabendo a ECT a aplicação de multa à ITAUTEC;
- Durante o PFE, os produtos que apresentarem defeitos, ou apresentarem mau funcionamento serão reparados ou substituídos imediatamente e, se dentro do conjunto composto por equipamentos do mesmo tipo, o número de equipamentos defeituosos

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 850
Doc. 3698

ultrapassar 10% (dez por cento) do seu total, todo o conjunto desse tipo de equipamento será substituído sem ônus para a ECT;

- Para os servidores INTEL de todos os tipos, a ITAUTEC executará, nos servidores indicados pela ECT, o software MS SYSTEM STRESS da MICROSOFT pelo período de 72 (setenta e duas) horas ininterruptas em cada equipamento. Caso o servidor apresente problemas de hardware durante este período, a ITAUTEC executará o reparo ou substituição e o teste será executado novamente. Caso o equipamento volte a apresentar defeito ou mau funcionamento em outras 2 (duas) tentativas, o equipamento será substituído sem ônus para a ECT;
- Para os servidores RISC TIPO 1, a ITAUTEC realizará teste de 'STRESS' dos componentes de processamento, memória e I/O. Os testes deverão proporcionar intensiva utilização do poder de processamento, alocação intensiva de memória RAM e componentes de I/O, devendo ainda realizar intensiva escrita e leitura no equipamento de Storage da ECT. A ITAUTEC, em estrita concordância com a ECT, poderá lançar mão de qualquer ferramenta que realize os testes especificados. O período de testes não será inferior a 24 (vinte e quatro) horas ininterruptas nos equipamentos apontados pela ECT. Caso o servidor apresente problemas de hardware durante este período, a ITAUTEC executará o reparo ou substituição e o teste será executado novamente. Caso o equipamento volte a apresentar defeito ou mau funcionamento em outras 2 (duas) tentativas, o equipamento será substituído sem ônus para a ECT;
- Serão também objetos de avaliação pela ECT o atendimento, suporte, execução dos serviços, bem como os planos de Treinamento;
- A equipe de implantação da ITAUTEC permanecerá alocada e presente durante o prazo de 30 (trinta) dias após emitido o Termo de Aceitação da Fase III.

1.5. DISPONIBILIDADE

- Os produtos estarão disponíveis 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;
- Os valores mínimos de disponibilidade para cada produto, apurados mensalmente, serão de 98,33%, (noventa e oito virgula trinta e três por cento);
- A disponibilidade de cada produto será calculada para o período de 30 (trinta) dias corridos, pela seguinte operação:

  $D = [(To - Ti)/To] * 100\%$

  onde: D = disponibilidade (em %);

  To = período de operação (últimos 30 dias corridos) em minutos;

  Ti = somatório dos minutos com interrupções do serviço durante os últimos 30 (trinta) dias corridos de operação).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 851
Doc.

- Sempre que forem apurados valores de disponibilidade mensais abaixo dos valores mínimos estabelecidos, será calculado o período (tempo) de indisponibilidade do serviço, que será o somatório dos tempos de indisponibilidade, desde a zero hora do primeiro dia até as vinte e quatro horas do último dia do mês corrente;
- No cálculo de disponibilidade não serão computadas as interrupções previamente acordadas entre a ITAUTEC e ECT.

1.6. COMPATIBILIDADE E PORTABILIDADE

- A ITAUTEC garante que os produtos referentes aos servidores RISC Tipo 1, devem ser compatíveis com os softwares relacionados a seguir:
  - ✓ Softwares

1) Aplicação OneWorld JDEdwards XE;
2) Servidor de Aplicação Websphere Application Server v 4.0;
3) Banco de Dados Oracle v 9i - 64 bits.

- A ITAUTEC deve responsabilizar-se, a qualquer tempo da vigência do contrato, pelas correções e customizações dos produtos fornecidos para a plataforma de servidores RISC. Ficando a cargo da ECT as correções ou customizações das Aplicações Corporativas (aplicativos) migrados para os equipamentos RISC fornecidos.

1.7. GARANTIA E ASSISTÊNCIA TÉCNICA

- Todos os produtos fornecidos possuem garantia de funcionamento durante a vigência do Contrato;
- A garantia e a assistência técnica cobrirão as localidades de Brasília/DF e São Paulo/SP, quer seja através de filiais da própria empresa, quer seja através de representantes credenciados;
- A garantia e a assistência técnica de todos os produtos abrangem a manutenção preventiva e corretiva de defeitos apresentados, inclusive substituição de peças, partes, componentes e acessórios fornecidos;
- A manutenção corretiva é a série de procedimentos executados, mediante solicitação da ECT, para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;
- Os serviços de manutenção corretiva serão prestados nas dependências da ECT, onde se encontrarem instalados os produtos. Esses serviços de manutenção corretiva serão executados pela ITAUTEC, a pedido da ECT;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 12
Fls. Nº 852
Doc. 3690

- A ITAUTEC não deixará de executar a manutenção corretiva sob qualquer alegação, mesmo sob pretexto de não ter sido executada anteriormente qualquer tipo de intervenção no respectivo produto, quer seja tal intervenção a limpeza externa, a manutenção preventiva ou qualquer outra;
- Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, deslocamento, embalagem, peças, partes, manuais do fabricante, será de inteira responsabilidade da ITAUTEC, não devendo gerar qualquer ônus à ECT;
- A ITAUTEC poderá prestar os serviços de manutenção através de empresas credenciadas, desde que os interventores técnicos dessas credenciadas também tenham habilitação legal e técnica, as quais serão apresentadas, à ECT, na ocasião da manutenção. Tais habilitações também poderão ser solicitadas a qualquer momento pela ECT.
- A ITAUTEC será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à ECT ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do contrato;
- O tempo de atendimento para efeito de aplicação de penalidades decorrentes do não cumprimento dos prazos de atendimento aos chamados técnicos será contabilizado a partir do registro da ocorrência pela ECT;
- A ITAUTEC se compromete a substituir, sem ônus para a ECT, os produtos instalados por novos com as mesmas especificações, funcionalidades e capacidade dos contratados, durante a vigência do Contrato, sempre que forem enquadrados em qualquer uma das seguintes situações:
  - ✓ Produtos que apresentarem 2 (dois) ou mais defeitos que comprometam o seu funcionamento e desempenho, dentro de um período de 30 (trinta) dias;
  - ✓ quando a soma dos tempos de paralisação do produto ultrapassar 20 (vinte) horas, dentro de um período de 30 (trinta) dias.
- A substituição de que trata a alínea anterior ocorrerá no prazo de 10 (dez) dias corridos, a partir do registro da ocorrência pela ECT;
- A ITAUTEC possui, ela mesma ou seus representantes, estoques de peças e componentes dos equipamentos fornecidos nas cidades de Brasília/DF e São Paulo/SP;
- A ITAUTEC apresentará DECLARAÇÃO de que manterá por no mínimo 5 (cinco) anos peças em estoque para os PRODUTOS fornecidos;
- A ITAUTEC manterá por no mínimo 5 (cinco) anos peças em estoque para os PRODUTOS fornecidos (vide Anexo 2);

1.8. CHAMADOS TÉCNICOS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 13
Pág. 13
Doc. 3698

- Todas as demandas, inclusive as que resultem em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, serão documentados por sistema informatizado de gerenciamento do Serviço de Atendimento/Suporte Técnico;
- A cada chamado técnico a ITAUTEC emitirá, por escrito, ordem de serviço discriminando os seguintes itens: o número identificador do chamado, a data e a hora do chamado, a data e a hora do atendimento, o motivo da chamada, causa do defeito, a situação do chamado, a data e a hora da solução, os trabalhos executados, a marca, modelo, número de série do equipamento, o técnico executante da solução definitiva e as peças substituídas, tudo de forma clara, compreensível e facilmente legível;
- Todas as informações relativas aos chamados técnicos serão disponibilizadas à ECT através de relatórios mensais de acompanhamento, a serem entregues em cópia impressa e em mídia eletrônica, até o 5º (quinto) dia útil do mês subseqüente;
- A ITAUTEC apresentará e fornecerá ao empregado da ECT, responsável pelo acompanhamento do chamado, logo após a conclusão do mesmo, a ordem de serviço mencionada no item anterior, para aceite e atesto;
- Mesmo se permitir pela ECT, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não representará qualquer ônus adicional à ECT;
- A ECT permitirá o acesso dos técnicos credenciados pela ITAUTEC às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da ECT, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;
- As interrupções programadas para manutenções preventivas dos equipamentos contratados serão comunicadas à ECT com antecedência mínima de 5 (cinco) dias úteis. O horário será negociado de forma a não haver impacto na produção;
- A ITAUTEC disponibilizará à ECT um serviço de atendimento com discagem gratuita (0800) ou qualquer outro meio de comunicação de disponibilidade imediata, sem ônus para a ECT, para chamada do serviço de suporte técnico que estará acessível durante 24h x 7 x 365 (vinte e quatro horas por dia, sete dias na semana, trezentos e sessenta e cinco dias por ano).

1.8.1. CHAMADO DE SUPORTE DE HARDWARE

- Com atendimento "on site" (atuação de um técnico no local onde está instalado o equipamento), no prazo máximo de 02 (duas) horas. O Prazo máximo para restauração do equipamento inoperante é de até 06 (seis) horas e o prazo máximo para solução total do problema é de até 12 (doze) horas. Todos os prazos serão contabilizados a partir do registro de ocorrência pela Empresa Brasileira de Correios e Telégrafos . A solução do problema engloba a substituição por outro equipamento com capacidade similar ou superior, até o conserto integral do equipamento com defeito, caso o reparo não seja possível dentro do prazo acima;

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 85
3698
Doc.

- A ITAUTEC disponibilizará à ECT um serviço de atendimento com discagem gratuita (0800) ou qualquer outro meio de comunicação de disponibilidade imediata, sem ônus para a ECT, para chamada do serviço de suporte técnico que estará acessível durante 24h x 7 x 365 (vinte e quatro horas por dia, sete dias na semana, trezentos e sessenta e cinco dias).

1.8.2. CHAMADO DE SUPORTE DO AMBIENTE OPERACIONAL

- Com atendimento "on site" (atuação de um técnico no local onde está instalado o ambiente operacional), no prazo máximo de 02 (duas) horas. O prazo máximo para restauração das funcionalidades inoperantes é de até 06 (seis) horas e o prazo máximo para solução total do problema é de até 12 (doze) horas. Todos os prazos serão contabilizados a partir do registro de ocorrência pela ECT.
- Os prazos estabelecidos acima não se referem a BUGS de software que necessitem de apoio de laboratório do fabricante. Nestes casos os prazos serão definidos e acordados pela ECT em conjunto com a ITAUTEC.
- Entende-se como AMBIENTE OPERACIONAL todos os softwares instalados ou embarcados nos equipamentos, tais como e não se limitando a: sistemas operacionais, softwares de backup, ferramentas de gerência, microcódigo, bios e firmware.

1.8.3. HORÁRIO DE ATENDIMENTO DE SUPORTE

- A ITAUTEC disponibilizará de estrutura que permita o registro de ocorrência pela ECT e atendimento de suporte em horário integral, sendo 24h x 7 x 365 (vinte e quatro horas por dia, sete dias na semana, trezentos e sessenta e cinco dias por ano).

1.9. TREINAMENTO

1.9.1. TREINAMENTO OPERACIONAL

- A ITAUTEC ministrará WORKSHOPS, com 2 (duas) turmas de até 12 (doze) participantes cada, sendo 1 (uma) turma em Brasília e 1 (uma) turma em São Paulo.
- Os WORKSHOPS serão realizados em locais disponibilizados pela ITAUTEC nas cidades de Brasília e São Paulo, próximo aos locais de instalação dos produtos.
- Cada WORKSHOP deve abordar os itens citados abaixo, sendo que a carga horária de cada um será negociada previamente com a ECT, de forma a permitirá aos técnicos da ECT o conhecimento pleno dos seguintes itens:
- Conectividade
  - ✓ Topologia e equipamentos da rede TCP/IP (Switches e Roteadores)
  - ✓ Operação dos softwares de gerenciamento da rede TCP/IP
- Rede SAN e Backup

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 15
Doc.

- ✓ Características dos equipamentos e política de backup implantada
- ✓ Topologia e equipamentos da rede SAN
- ✓ Operação dos equipamentos de Backup
- ✓ Operação dos softwares de gerenciamento da Rede SAN e do Backup
- ✓ Geração de relatórios de estatísticas de utilização dos equipamentos

- Servidores RISC e INTEL
  - ✓ Características dos equipamentos
  - ✓ Implementação e operação do particionamento lógico/físico
  - ✓ Implementação e operação do Gerenciamento de pré-falha dos Servidores
  - ✓ Implementação do ambiente de alta disponibilidade em RISC
  - ✓ Implementação do ambiente de alta disponibilidade em INTEL

- Equipamentos de Segurança Lógica
  - ✓ Características dos equipamentos e softwares envolvidos no ambiente de segurança
  - ✓ Operação dos softwares utilizados na segurança lógica
  - ✓ Configuração de regras, restrições e políticas nos equipamentos de segurança lógica
  - ✓ Definição, configuração e geração de relatórios

- Chamados Técnicos
  - ✓ Características do contrato de garantia dos PRODUTOS
  - ✓ Check-list de ocorrências mais comuns e soluções
  - ✓ Verificações mínimas antes de acionar o suporte
  - ✓ Levantamento das informações necessárias para abertura de chamado técnico
  - ✓ Contatos com a ITAUTEC para suporte e manutenção.

- A ITAUTEC entregará, a cada participante, em cada workshop realizado, material didático elaborado de acordo com o assunto a ser abordado. O material será entregue a ECT, 15 (quinze) dias antes da realização de cada workshop para avaliação quanto aos padrões de qualidade estabelecidos pela ECT.
- No material a ser entregue estará inserido todo o assunto abordado durante o workshop, devendo ainda estar previsto espaço para anotações de itens relevantes. Serão exigidas boa edição, impressão e encadernação para todo o material fornecido. A impressão a cores será exigida sempre que for indicada para melhor visualização de gráficos, desenhos, tabelas e fotos.

RQS nº 03/2005 - CN
CORREIOS
Pág. 16
Fls. Nº 358
Doc.

- Todas as despesas com material, impressão e encadernação serão por conta da ITAUTEC.
- As datas de realização dos WORKSHOPS serão negociadas com a ECT, no mínimo, 5 (cinco) dias úteis antes da realização do referido workshop, de forma a permitir a disponibilidade dos participantes.
- À ECT resguardar-se-á o direito de acompanhar e avaliar os workshops, com instrumento próprio de avaliação.

1.9.2. TREINAMENTO ON-SITE

- A Equipe de Projeto da ITAUTEC realizará a passagem de conhecimento sobre os produtos e a arquitetura implantada para os profissionais que irão atuar no treinamento on-site. A duração desta transferência de conhecimento não será inferior a 30 (trinta) dias a partir da data do aceite da FASE III.
- A ECT solicitará, a qualquer momento da vigência do Contrato, a seu critério, a substituição de qualquer membro da equipe de treinamento, comprometendo-se a comunicar com antecedência de 15 (quinze) dias;
- A ITAUTEC alocará profissionais nas instalações da Empresa Brasileira de Correios e Telégrafos, nas cidades de Brasília/DF e São Paulo/SP, para realizar a transferência de tecnologia, através de treinamentos práticos, nas 4 (quatro) especialidades descritas abaixo.

1.9.2.1. TREINAMENTO DE HARDWARE

- A ITAUTEC alocará e manterá, sem gerar ônus à ECT, 02 (dois) profissionais especializados em atendimento de hardware, nas dependências da ECT, sendo 01 (um) no CCD de Brasília e 01 (um) no CCD de São Paulo.
- Estes profissionais estarão presentes em cada CCD, nas cidades de Brasília/DF e São Paulo/SP, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, estando disponíveis para consultas através de celular ou pager nos demais dias e horários.
- Os profissionais realizarão a transferência de conhecimento da tecnologia e da operação do hardware fornecido pela ITAUTEC.
- O treinamento ocorrerá durante o período de 6 (seis) meses a partir da data do aceite da FASE III.

1.9.2.2. TREINAMENTO DE SOFTWARE

- A ITAUTEC alocará e manterá, sem gerar ônus à ECT, 02 (dois) profissionais especializados em atendimento de software, nas dependências da ECT, sendo 01 (um) profissional no CCD de Brasília e 01 (um) profissional no CCD de São Paulo

RQS nº 03/2005 - CN CPMI - CORREIOS
Pág. 17
Fls. Nº 857
Doc.

- Estes profissionais estarão presentes em cada CCD, nas cidades de Brasília/DF e São Paulo/SP, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, estando disponíveis para consultas através de celular ou pager nos demais dias e horários.
- Os profissionais realizarão a transferência de conhecimento da tecnologia e da operação dos softwares fornecido pela ITAUTEC.
- Os profissionais designados pela ITAUTEC possuirão conhecimentos técnicos aprofundados, das seguintes especialidades:
  - ✓ Sistemas Operacionais Unix em Alta Disponibilidade;
  - ✓ Análise de Performance de Sistemas Operacionais Unix;
  - ✓ Unidades de Backup;
  - ✓ Gerenciadores de Backup;
  - ✓ Redes SAN.
- Estes conhecimentos estarão atualizados nas versões/modelos dos produtos fornecidos pela ITAUTEC.
- Os profissionais serão apresentados, pelo menos 15 (quinze) dias antes do início do treinamento de software, munidos de currículo com os respectivos certificados para entrevista e análise pela equipe técnica da ECT.
- O treinamento ocorrerá durante o período de 48 (quarenta e oito) meses a partir da data do aceite da FASE III.

1.9.2.3. TREINAMENTO DE GERENCIAMENTO

- A ITAUTEC alocará e manterá, sem gerar ônus à ECT, 1 profissional especializado em gerenciamento nas dependências da ECT, no CCD de Brasília-DF.
- Este profissional estará presente no CCD, na cidade de Brasília-DF, das 8:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, estando disponível para consultas através de celular ou pager nos demais dias e horários.
- Este profissional realizará a integração dos PRODUTOS fornecidos à Plataforma de Gerenciamento da ECT, repassando aos técnicos da mesma os detalhes técnicos necessários à integração.
- O profissional poderá, a critério da ECT, ser convocado a realizar os trabalhos de integração das ferramentas no CCD/SPM, na cidade de São Paulo-SP. Todas as despesas relativas a passagens, alimentação e estadas serão de responsabilidade da ITAUTEC.
- O profissional designado pela ITAUTEC, possuirá conhecimentos técnicos aprofundados, no mínimo, das seguintes especialidades:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 858
Doc.

- ✓ Implantação de Gerenciamento de Ambiente de Produção baseado na Plataforma HP OpenView (Network Node Manager – NNM e OpenView Operations – OVO);
- ✓ Implantação de Gerenciamento de Ambiente de Produção baseado na Plataforma Concord eHealth.

- O profissional terá participado da elaboração e implantação de projetos de gerenciamento utilizando as duas plataformas mencionadas, HP OpenView e Concord eHealth, em pelo menos, 3(três) empresas de médio/grande porte.
- A participação nestes projetos será comprovada através de declarações emitidas pelas empresas nas quais os projetos foram desenvolvidos ou pelas empresas pelas quais o profissional prestou os serviços.
- O profissional possuirá treinamento oficial nas principais ferramentas das plataformas mencionadas, HP OpenView e Concord eHealth, especificamente, NNM e OVO.
- O profissional será apresentado, pelo menos 15 (quinze) dias antes do início do treinamento de gerenciamento, munido de currículo com os respectivos certificados e declarações, para entrevista e análise pela equipe técnica da ECT.
- O treinamento ocorrerá durante o período de 48 (quarenta e oito) meses a partir da data do aceite da FASE III.

1.9.2.4. TREINAMENTO DE SUPORTE

- A ITAUTEC alocará e manterá, sem gerar ônus à ECT, 4 (quatro) profissionais especializados no atendimento de suporte técnico, nas dependências da ECT, sendo 02 (dois) profissionais no CCD de Brasília e 02 (dois) profissionais no CCD de São Paulo.
- Estes profissionais estarão presentes em cada CCD, nas cidades de Brasília-DF e São Paulo, das 08:00 às 18:00h, com intervalo de até 2 (duas) horas, de segunda a sexta, estando disponíveis para consultas através de celular ou pager nos demais dias e horários.
- Cada profissional, mediante solicitação da ECT, poderá ser convocado a trabalhar fora do horário pré-determinado até o limite de 32 (trinta e duas) horas extras por mês, cabendo a ITAUTEC os encargos financeiros e trabalhistas resultantes destas convocações.
- O conjunto formado por estes profissionais possuirá, no mínimo, treinamento oficial dos fabricantes dos softwares e hardware, nos modelos e versões fornecidos pela ITAUTEC. A capacitação dos profissionais permitirá a resolução de problemas relacionados as seguintes especialidades:
  - ✓ Sistemas Operacionais Unix em Alta Disponibilidade;
  - ✓ Sistemas Operacionais Windows em Alta Disponibilidade;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc.

- ✓ Unidades de Armazenamento e Backup;
- ✓ Gerenciadores de Backup e Redes SAN;

- Estes conhecimentos estarão atualizados nas versões/modelos dos produtos fornecidos pela ITAUTEC.
- Os profissionais serão apresentados, pelo menos 15 (quinze) dias antes do início do treinamento de suporte, munidos de currículo com os respectivos certificados para entrevista e análise pela equipe técnica da ECT. Caso sejam considerados com perfil técnico ou profissional inadequado, serão substituídos pela ITAUTEC, sem qualquer ônus para a ECT.
- Os diplomas serão emitidos por centros de formação autorizados pelos fabricantes/desenvolvedores dos equipamentos e softwares fornecidos pela ITAUTEC.
- O treinamento ocorrerá durante o período de 48 (quarenta e oito) meses a partir da data do aceite da FASE III.

1.9.3. TREINAMENTO OFICIAL

- Os cursos serão ministrados por Instrutores Certificados pelo fabricante/desenvolvedor dos produtos;
- O treinamento poderá ocorrer pelo período de até 24 (vinte e quatro) meses, a partir do aceite da FASE III;
- Os cursos serão ministrados por Instrutores Certificados pelo fabricante/desenvolvedor dos produtos fornecidos;
- A grade de cursos será elaborada pela ITAUTEC de forma a atender os valores mínimos especificados para cada item:
- Formação de Especialista em Sistemas Operacionais Microsoft
  - ✓ 160 horas-aula por aluno;
  - ✓ 4 (quatro) turmas com 6 (seis) alunos cada, sendo 3 (três) turmas em Brasília e (uma) turma em São Paulo.
- Formação de Especialista em Sistemas Operacionais UNIX
  - ✓ 160 horas-aula por aluno;
  - ✓ 4 (quatro) turmas com 6 (seis) alunos cada, sendo 3 (três) turmas em Brasília e 1 (uma) turma em São Paulo.
- Formação de Administradores de Banco de Dados MS SQL SERVER 2000
  - ✓ 80 horas-aula por aluno;
  - ✓ 2 (duas) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 860
Doc.

Itautec

- Formação de Especialista em Segurança Lógica
  - ✓ 160 horas-aula por aluno;
  - ✓ 2 (duas) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília ou São Paulo ou Rio de Janeiro
- Formação de Especialista em Conectividade - Switches TCP/IP e Roteadores
  - ✓ 220 horas-aula por aluno;
  - ✓ 3 (três) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília e 1 (uma) turma em São Paulo.
- Formação de Especialista nas Ferramentas de Gerenciamento
  - ✓ 80 horas-aula por aluno;
  - ✓ 3 (três) turmas com 6 (seis) alunos cada, sendo 2 (duas) turmas em Brasília e 1 (uma) turma em São Paulo.
- As turmas serão prioritariamente fechadas. O Treinamento poderá ser realizado em Turmas abertas, caso as datas coincidam com as datas definidas pela ECT.
- A ITAUTEC apresentará a grade detalhada com proposta de cronograma dos treinamentos oficiais para validação pela ECT.
- A ITAUTEC ministrará todos os treinamentos tendo como idioma o português (Brasil).
- A ITAUTEC fornecerá ao final de cada conjunto de cursos oficiais, as provas de certificação, em Centros Autorizados na cidade de Brasília. As certificações mínimas que serão oferecidas são as seguintes:
- Plataforma INTEL (12 vagas)
  - ✓ MICROSOFT – Microsoft Certified System Administrator – MCSA
- Plataforma RISC* (12 vagas)
  - ✓ IBM – AIX System Administration

  * será ofererecerida a prova para a plataforma RISC ofertada (IBM).
- Conectividade (12 vagas)
  - ✓ Serão fornecidas as provas de acordo com o programa de certificação de fabricante de equipamentos de rede, prevendo nível de especialista em switches e roteadores.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 21
Fls Nº 861
Doc.

Itautec

2. Descrição dos Serviços

2.1 Instalação de Infra Elétrica para a Sala Cofre

Escopo

Implementar as adequações necessárias nos elementos e subsistemas das Salas de Segurança Física dos sites de Brasília e São Paulo, visando a instalação de novos equipamentos de informática.

Procedimentos de Montagem Geral

Para a execução dos serviços, a ITAUTEC seguirá as normas aplicáveis da ABNT, bem como as práticas usuais consagradas para a execução dos serviços.

Observações

A ITAUTEC, antes de executar quaisquer serviços, se reunirá com a contratante para a obtenção de informações visando a prevenção de riscos de quaisquer natureza decorrentes das particularidades locais para os serviços a serem executados e das interfaces com outras disciplinas.

Modificações e Atualização de Plantas

Todas as alterações nos projetos, quando da execução dos serviços, serão assinaladas em AS-BUILT.

Requisitos e responsabilidades

- Fornecimento de todos equipamentos e materiais desta adequação.
- Gerenciamento das intervenções necessárias para a adequação.
- Transporte, instalação, montagem, remoções e limpeza.
- 48 (quarenta e oito) meses de suporte técnico e manutenção.
- Assistência técnica para início das operações, instruções dos usuários.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 862
Doc.

- Documentação operacional, manuais e desenhos das adequações.
- Declaração da extensão de garantia do fabricante da sala e sua solidariedade com o proponente sobre as adequações efetuadas e que esta mantém suas características de estanqueidade, além de manter a disposição peças de reposição por 5(cinco) anos a partir da data finalização das adaptações.
- Recolhimento de todas taxas e impostos de acordo com as leis vigentes nesta data.

Para todo fornecimento devem ser mantidas as características e fabricantes dos equipamentos e materiais já instalados, de forma a uniformizar e preservar as características originais de segurança e desempenho dos conjuntos.

Escopo das intervenções

Antes do início das atividades, será agendado junto ao cliente uma reunião para definições de cronograma e a estratégia a ser adotada, visando a prevenção de riscos de quaisquer natureza decorrentes das particularidades dos sistemas locais, dos serviços a serem executados e das interfaces com outras disciplinas.

Intervenção dos sistemas principais:

- Devem ser executadas intervenções nas Salas de Segurança Física, dotando-as de novas aberturas e instalação de blindagens para cabos e tubulações, estas intervenções serão efetuadas por pessoal especializado para não haver prejuízos a segurança e "estanqueidade" das salas de segurança.
- A especialidade será comprovada através da carta de solidariedade e exclusividade do fabricante.
- Fornecimento de expansão do sistema de detecção precoce de incêndio, para complementação do sistema em virtude do complemento do sistema de climatização da Sala de Segurança;
- Integração dos novos equipamentos aos sistemas de detecção precoce de incêndio, controle e monitoramento ambiental existentes, de modo a manter as características e performance de atuação sem prejuízos ao sistema já instalado.

Quadros gerais de distribuição dos No-Breaks, Barramento Seguro (QDX e QDY)

Estes quadros serão complementados com a instalação de novos disjuntores para alimentação de novos painéis de distribuição interna da sala de segurança física, no mesmo padrão e funcionalidade dos atuais.

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 863
Doc.

Itautec

Quadros auto portantes da Sala Cofre (QdiX2 , QdiY2) em São Paulo e (QdiX2, QdiY2 , QdiX3 e QdiY3) em Brasília

Os quadros a serem instalados, seguirão o mesmo padrão existente, dotados de disjuntores extraíveis (plug-in) com tampa transparente em policarbonato.

Serão contemplados um total de 108 (cento e oito) circuitos duais, totalizando 216 (duzentos e dezesseis) pontos elétricos no ECT Brasília e 65 (sessenta e cinco) circuitos duais, totalizando 130 (cento e trinta) pontos elétricos no ECT São Paulo.

Todos os quadros seguirão o padrão dos quadros atuais como fabricante e linha de disjuntores, medições e outras características.

Eletrocalhas

A interligação entre os quadros QDX e QDY será executada através das eletrocalhas existentes.

A infra estrutura sob o piso elevado das salas será em leitos aramados em inox, com os devidos acessórios de derivação e fixação e identificações no padrão existente.

Serão instaladas tomadas para alimentação dos equipamentos, estações de trabalhos e outras cargas da sala cofre. Serão instaladas duas réguas de tomadas em cada rack a partir do QdiX2 , QdiY2 em São Paulo e QdiX2 ,QdiY2 , QdiX3 e QdiY3 em Brasília .

Sistema de Cabeamento lógico

São Paulo

Cabeamento Horizontal UTP: instalação de 6000 metros de UTP 4 pares cat. 6 para atender os 180 pontos estruturado, sendo que os 180 pontos estão sendo considerados para atender as estações de trabalho e equipamentos dentro da sala cofre. Esses 180 pontos serão distribuídos de forma horizontal para atender cada estação de trabalho com 02 pontos, possibilitando serviços de (dados, voz, imagem etc.) em cada ponto, esses cabos seguirão por leitos aramados até os Racks a serem instalados conforme o lay out a ser definido.

Conectores UTP: Instalação de 180 conectores RJ-45 fêmea cat. 6 para terminação nas extremidades dos cabos UTP 4 pares do Cabeamento Estruturado .

Surface Box : Fornecimento e instalação de 90 Surface Box com 2 (duas) posições, para a instalação e identificação dos conectores RJ-45 fêmea nas estações de trabalho.

RQS nº 03/2005 - CN
CORREIOS
Pág. 24
Fls Nº 864
Doc. 3698

Itautec

Patch Panel UTP: Fornecimento e instalação de 8 patch panels 19'' com 24 portas cat. 6 dentro dos Racks a serem instalados, para terminação dos cabos UTP 4 pares provenientes das estações de trabalho.

Patch Cords UTP: Fornecimento e instalação de 180 patch cords de 1,5 metros para conexão de serviços de dados e voz nos Racks, referidos acima.

Fornecimento e instalação de 180 patch cords de 3,0 metros para conexão de serviços de dados nas estações de trabalho, referidos acima.

Organizador Horizontal: Fornecimento e instalação 20 organizadores horizontais de 19''x 1U de altura, para organização dos patch cords nos Racks.

Cabeamento Ópticos

Disponibilizarão um total de 128 fiber channel , com cordão dúplex SC/SC MM com 3 metros do SW até distribuidor óptico e 27 metros do distribuidor óptico até o equipamento para atender as necessidades de acréscimo no site ETC São Paulo.

Testes e Identificações: Execução de medições para efetuar testes em todos os cabos UTP cat 6 e Ópticos , com emissão de relatórios dos resultados e instalação de etiquetas para identificação de todo o cabeamento instalado.

Brasília

Cabeamento Horizontal UTP: instalação de 12000 metros de cabos UTP 4 pares cat 6 para atender os 400 pontos estruturado, sendo que os 400 pontos estão sendo considerados para atender as estações de trabalho e equipamentos dentro da sala cofre. Esses 400 pontos serão distribuídos de forma horizontal para atender cada estação de trabalho e equipamentos com 02 pontos, possibilitando serviços de (Dados Voz, Imagem etc.) em cada ponto, esses cabos seguirão por leitos aramados até os Racks a serem instalados conforme o lay out a ser definido.

Conectores UTP: Instalação de 400 conectores RJ-45 fêmea cat. 6 para terminação nas extremidades dos cabos UTP 4 pares do Cabeamento Estruturado nas estações de trabalho.

Surface Box : Fornecimento e instalação de 200 Surface Box com 2 posições, para a instalação e identificação dos conectores RJ-45 fêmea nas estações de trabalho.

Patch Panel UTP: Fornecimento e instalação de 17 patch panels 19'' com 24 portas cat. 6 dentro dos Racks a serem instalados, para terminação dos cabos UTP 4 pares provenientes das estações de trabalho.

Patch Cords UTP: Fornecimento e instalação de 400 patch cords de 1,5 metros para conexão de serviços de dados e voz nos Racks, referidos acima.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 865
Doc.

Itautec

Fornecimento e instalação de 400 patch cords de 3,0 metros para conexão de serviços de dados nas estações de trabalho, referidos acima.

Organizador Horizontal: Fornecimento e instalação de 40 organizadores horizontais de 19''x 1U de altura, para organização dos patch cords nos Racks.

Cabeamento Óptico

Serão disponibilizando um total de 256 fiber channel com cordão duplex SC/SC MM com 3 metros do SW até o distribuidor óptico e 27 metros do distribuidor óptico até os equipamentos para atender as necessidades no site do ECT Brasília .

Testes e Identificações: Execução de medições para efetuar testes em todos os cabos UTP e Ópticos instalados, com emissão de relatórios dos resultados e instalação de etiquetas para identificação de todo o cabeamento instalado.

Sistema de Climatização

Para o site de Brasília será necessário o complemento do sistema de climatização existente.

Serão fornecidos 2 novos equipamentos de climatização, de mesmas características e potência dos demais já instalados na Sala de Segurança.

As unidades devem insuflar o ar climatizado diretamente por baixo do piso técnico, retornando pelo ambiente via filtro (descartável) de alta eficiência (EU 4 ou ASHRAE 30%) na parte superior da máquina, assim resfriando os equipamentos eletrônicos em circuito fechado com ar altamente filtrado, sem risco de contaminação de outras atividades no prédio. As conexões de energia e de tubulação serão pela base, via o entre-piso. Toda manutenção será efetuada apenas via área frontal, permitirá instalação em conjunto. O ventilador deve ter motor com acoplamento direto e permitirá ajuste de rotação, adequado para pressão externa de 100 Pa. O gabinete deve ser de dupla chapa pintado de epóxi, com isolamento térmico e acústico.

Os condensadores serão do tipo Drycooler, com acionamento direto, ventiladores do tipo axial, controles para operação da bomba. Para rejeitar o calor correspondente, os trocadores serão construídos com tubos de cobre e aletas de alumínio e deve ainda possuir baixo nível de ruído, ser resistente à corrosão e possuir estrutura em seu gabinete em alumínio, e ter controle de velocidade, permitirá desta maneira atuar com diferentes pressões de condensação em função da temperatura externa.

Os equipamentos de climatização fornecidos devem ser integrados e programados seguindo as características de funcionalidade do ambiente, mantendo a lógica de revezamento e disponibilidade das maquinas reserva hoje em funcionamento.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 866
Doc.

Itautec

Estas programações devem ser efetuadas diretamente nos equipamentos sem uso de painéis auxiliares, utilizando o recurso de comunicação entre maquinas através de cabos UTP.

Os procedimentos de instalação e partida deverão seguir rigorosamente as instruções do fabricante, que emitirá o certificado de garantia após o comissionamento. Será exigida do proponente a apresentação de certificado de aprovação técnica emitida pelo fabricante.

Critério de Conclusão

Após a instalação dos materiais UTP e cabos ópticos e execução dos respectivos serviços contemplados nesta proposta, estes itens passarão por uma avaliação para conclusão dos serviços ora propostos.

Estes itens serão avaliados de acordo com as tabelas a seguir:

Item a ser verificado	Parâmetro avaliado	Forma de verificação	Resultados Esperados
a. CABLING:			
a.1. Links de Cabos UTP, ótico	Continuidade, Resistência DC, Comprimento, Capacitância, NEXT, Atenuação, ACR e Impedância,	Ferramenta: Equipamento do tipo Penta Scanner, OTDR	De acordo com as normas vigentes e parâmetros dos fabricantes,
	Identificação,	Inspeção visual,	Conforme acordo entre a ITAUTEC e o Cliente,
a.2. Racks e tomadas de superfície	Fixação	Inspeção visual,	Conforme acordo entre a ITAUTEC e o Cliente,
	Defeitos de fabricação	Inspeção visual,	Sem defeito,
	Identificação,	Inspeção visual,	Conforme acordo entre a ITAUTEC e o Cliente,

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 867
Doc.

Itautec

2.2 Implementação de Servswitch

Planejamento da instalação

Nesta etapa será realizado o planejamento físico que servirá como base para a implementação dos equipamentos de servswitches nos CCD - Centros Corporativos de Dados de Brasília e São Paulo.

Descrição dos serviços

Serão fornecidas 2 (duas) redes de comutação de teclado, vídeo e mouse, sendo 1 (uma) rede no CCD de Brasília-DF e 1 (uma) rede no CCD de São Paulo-SP, devendo atender a todos os servidores da plataforma INTEL fornecidos, incluindo servidores legados existentes na ECT ;

Instalação de 10 (dez) servswitches em Brasília e 6 (seis) em São Paulo em cada unidade dos CCD - Centros Corporativos de Dados de Brasília e São Paulo. E suas devidas configurações

O conjunto de equipamentos fornecidos para o CCD de Brasília disponibilizará um mínimo de 160 (cento e sessenta) portas de comutação, independente da quantidade de equipamentos que utilizarão para atingir este número, respeitando o número mínimo de 16 (dezesseis) portas por equipamento;

O número mínimo de servidores legados que serão atendidos pela rede de comutação no CCD de Brasília é o seguinte:

- 24 Servidores RISC da Marca SUN Microsystems;
- 48 Servidores da Plataforma INTEL.

O conjunto de equipamentos fornecidos para o CCD de São Paulo disponibilizarão um mínimo de 96 (noventa e seis) portas de comutação, independente da quantidade de equipamentos que utilizarão para atingir este número, respeitando o número mínimo de 16 (dezesseis) portas por equipamento;

O número mínimo de servidores legados que serão atendidos pela rede de comutação no CCD de São Paulo é o seguinte:

- 48 Servidores da Plataforma INTEL.

Será disponibilizado um conjunto de 8 consoles externos à sala de segurança física para Brasília e um conjunto de 4 consoles externos à sala de segurança física para São Paulo;

RQS nº 03/2005 - CN CPMI Pág. 28 CORREIOS Fls. Nº 868 Doc. 3698

As consoles serão independentes entre si, podendo acessar qualquer servidor, inclusive os servidores legados

As 12 (doze) consoles utilizarão monitores de vídeo que alcancem resolução de 1280x1024 60Hz com no mínimo com 17" (dezessete polegadas), policromático e DOT PITCH 0,28, mouse e teclado padrão ABNT2;

As consoles serão montadas fora das Salas de Segurança Física de Brasília e São Paulo, a uma distância de aproximadamente 50 (cinqüenta) metros.

Para a conexão dos servidores à rede de comutação, a ITAUTEC fornecerá todos os cabos e acessórios necessários a esta operação.

Os cabos de interligação dos equipamentos fornecidos ao computador terão comprimento possuirão o comprimento suficiente para interligar todos os equipamentos, entretanto, os cabos utilizados para conectar servidores legados devem ter comprimento mínimo de 15 (quinze) metros

Os cabos a serem oferecidos terão comprimento suficiente para permitir a conexão a qualquer servidor, considerando as características dos equipamentos

Os equipamentos utilizados na rede de comutação serão cascateados, de modo que, a partir de qualquer uma das consoles seja possível o acesso a qualquer equipamento conectado nas redes de comutação

O servidor de comutação será configurado por menu, utilizando os nomes dos servidores designados pela ECT

Critério de Conclusão

Esta etapa estará concluída quando todos os equipamentos interligados nos servswitches estiverem configurados e em funcionamento do CCD Centros Corporativos de Dados de Brasília e São Paulo.

Exigências Especiais

Recomendações para instalação de equipamento

O fornecimento de tensão para os equipamentos ligados à rede deve ser de 220 V ou 120 V (dependendo do equipamento) com tolerância de +6% e - 8%.

A ligação de outros equipamentos, que não são de processamento de dados na mesma alimentação que atende aos equipamentos da rede pode gerar ruídos que afetam o funcionamento dos mesmos. Em função disto, recomenda-se que para estes equipamentos seja utilizada uma rede exclusiva, e também, o uso de tomadas que não permitam o uso indevido desta alimentação por outros tipos de equipamentos tais como aspiradores de pó ou ventiladores.

A qualidade da energia fornecida pode fazer uma grande diferença no desempenho dos equipamentos. Distúrbios ou interferências podem ocasionar falhas ou erros. Falhas

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº
Doc.

intermitentes podem se originar da companhia de fornecimento de força, mas são mais comumente causadas por equipamentos elétricos instalados no prédio ou local próximo. Por exemplo, intermitências podem ser causadas por motores, elevadores, máquinas de cópia ou outros equipamentos de escritório. O melhor modo para prevenir problemas causados por distúrbios de força é instalar um No-Break. Como segunda alternativa, menos eficaz, pode-se usar um estabilizador.

A impedância da malha de aterramento da rede será menor ou igual a 3 ohms, em qualquer época do ano.

O aterramento dos equipamentos ligados à rede será feito através de um condutor exclusivo e isolado, indo da malha até o barramento do quadro de distribuição de força. Salientamos que esta malha será interligada a outras malhas existentes.

Programa de Implantação

A seguir é apresentado um programa para o conjunto de atividades desta etapa do Projeto.

Entrega de Materiais: O prazo de entrega dos materiais está estimado em **30 (trinta) dias** após a definição final do cronograma de entrega.

Execução dos Serviços: O prazo para finalização dos serviços de cabling e elétrica está estimado em **90 (noventa) dias** após a entrega dos materiais e após a disponibilização por parte da ECT da infra-estrutura necessária para iniciar a instalação.

Os serviços necessários para realização deste projeto, objeto deste contrato, serão executados no horário de segunda a sexta-feira de 08:00 as 17:00 h.

Itens a serem entregues pela ITAUTEC

Documentação Técnica

Será fornecido à ECT o "As Built" desta etapa do Projeto em até 30 dias após a conclusão dos serviços.

Acompanhando o "As Built" será fornecido à ECT todos os resultados dos testes realizados no cabeamento ótico, obedecendo as Normas pertinentes, certificando que estão adequados e aptos para utilização.

Consideramos que serão fornecidas pela ECT as plantas baixas dos locais de instalação em arquivos de AUTOCAD, incluindo a infra-estrutura para a passagem dos cabos.

No escopo do trabalho de cabeamento, estão incluídos os seguintes itens de serviço:

- Fornecimento e instalação dos materiais.
- Identificação de todos os cabos UTP e Óptico descrito nesta proposta conforme padrão ITAUTEC.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 870
Doc. 3608

Itautec

- Testes do cabeamento UTP.
- Não estão incluídos os seguintes itens de fornecimento:
- Fornecimento e instalação de qualquer infra-estrutura civil (por exemplo, eletrodutos, leitos para fios e cabos e seus acessórios).
- Fornecimento e instalação de qualquer infra-estrutura elétrica ou de refrigeração adicional ao escopo desta etapa.

Programação de entrega e local onde os itens acima serão entregues

Todas as documentações serão fornecidas à ECT, ao Gerente de Projeto da ECT ou a quem o mesmo indicar.

Outros termos não especificados anteriormente

O não cumprimento de quaisquer itens desta proposta, durante a execução dos serviços, por parte da ECT, implicará na paralisação dos mesmos, até que se satisfaçam as exigências do item não cumprido, sendo que o prazo de execução será acrescido de tantos quantos forem os dias de paralisação, mais o necessário para a nova mobilização.

Garantia

Uma vez concluídas, todas as instalações são garantidas pelo prazo especificado abaixo contra defeitos comprovados de execução, a contar da data da entrega das instalações.

A garantia descrita compreende os reparos necessários durante o período mencionado, desde que a instalação seja mantida em operação, de forma adequada.

A garantia é intransferível, beneficiando apenas à ECT, durante o prazo de garantia.

Para esse fim, ao término das obras, a ITAUTEC entregará à ECT, se existentes, todas as garantias escritas, correspondentes a esses produtos, bem como manuais de manutenção e/ou utilização.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 3698
Fls Nº 871
Doc.

2.3 Implementação da Conectividade da Rede

Planejamento da instalação

Nesta etapa será realizado o planejamento físico e lógico que servirá como base para a implementação dos switches Tipo 1, 2, e 5, Roteadores Tipos 1 e 2, Servidores de Segurança Lógica Tipo 1 e Tipo 2, e Sistema para Detecção de Intrusão dos CCD - Centros Corporativos de Dados de Brasília e São Paulo. Tendo como base os endereços da rede atual e a política de os parâmetros de segurança de rede já implementados, estaremos fazendo, em conjunto com a ECT o endereçamento IP, a definição das VLANs, dos parâmetros de roteamento e segurança a serem implementados na ampliação da estrutura dos CCD - Centros Corporativos de Dados de Brasília e São Paulo.

Critério de Conclusão

Esta etapa estará concluída quando da entrega do projeto de endereçamento físico e lógico dos switches, roteadores e servidores de segurança for feito pela ITAUTEC à ECT.

OBS: Para o sucesso desta etapa é primordial a participação do corpo técnico da ECT responsável pela rede e segurança de rede com os parâmetros de endereço e segurança atualmente em uso.

Instalação do Switch Tipo 1 em Brasília e em São Paulo

Atividades a serem realizadas:

- Quantidade: 2 equipamentos Cisco modelo Catalyst 6513 em Brasília
- Quantidade: 2 equipamentos Cisco modelo Catalyst 6513 em São Paulo;
- Desembalagem;
- Montagem dos Módulos;
- Montagem do equipamento no Rack;
- Ligação e teste;
- Configuração (SNMP, IP, VLANs, roteamento e gerenciamento);
- Configuração do balanceamento de carga;
- Testes operacionais.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0682
Doc. 3698

Itautec

Critério de Conclusão

Esta instalação estará concluída quando houver comunicação entre a rede existente e a rede nova. A configuração do Switch deverá permitir que as estações de trabalho que estejam em perfeito funcionamento e com a configuração de endereçamento TCP/IP coerente com o determinado pelo projeto de endereçamento da rede possam realizar comunicação através do protocolo TCP/IP, o que será demonstrado pela execução de um comando PING de uma estação ao Switch e aos servidores da rede.

Instalação do Switch Tipo 2 em Brasília e em São Paulo

- Quantidade: 4 equipamentos Cisco modelo Catalyst 2950 em Brasília
- Quantidade: 2 equipamentos Cisco modelo Catalyst 2950 em São Paulo
- Desembalagem;
- Montagem do equipamento no Rack;
- Montagem das fontes redundantes;
- Montagem dos GBICs para empilhamento;
- Ligação e teste;
- Configuração (SNMP, IP de gerenciamento e VLANs,);
- Configuração da conexão com a rede existente;
- Testes operacionais.

Critério de Conclusão

Esta instalação estará concluída quando houver comunicação entre a rede existente e o switch instalado. A configuração do Switch deverá permitir que as estações de trabalho que estejam em perfeito funcionamento e com a configuração de endereçamento TCP/IP coerente com o determinado pelo projeto de endereçamento da rede possam realizar comunicação através do protocolo TCP/IP, o que será demonstrado pela execução de um comando PING de uma estação ao Switch e aos servidores da rede.

Instalação do Switch Tipo 5 em Brasília e em São Paulo

- Quantidade: 1 conjunto de alta disponibilidade(2 equipamentos) CVPN3060 em Brasília
- Quantidade: 1 conjunto de alta disponibilidade(2 equipamentos) CVPN3060 em São Paulo
- Desembalagem;
- Ligação e teste;

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 873
Doc.

- Configuração (SNMP, IP, VLANs, VPNs);
- Testes operacionais.

Critério de Conclusão

Esta instalação estará concluída quando houver comunicação através de um túnel VPN formado entre a rede da ECT e a rede de suporte da ITAUTEC em Tutóia ou outra rede, na impossibilidade de link entre os sites. A configuração do Switch deverá permitir que as estações de trabalho que estejam em perfeito funcionamento, com o software VPN client instalados(a ITAUTEC instalará em 2 maquinas com conectividade direta a Internet) e com a configuração de endereçamento TCP/IP coerente com o determinado pelo projeto de endereçamento da rede possam realizar comunicação através do protocolo TCP/IP, o que será demonstrado pela execução de um comando PING de uma estação a um dos servidores da rede. Após a instalação do Switch, o software de gerenciamento de VPN's poderá colher informações sobre as VPN's configuradas no equipamento.

Instalação do Roteador Tipo 1 em Brasília e em São Paulo

- Quantidade: 1 equipamento Cisco modelo 3745 em Brasília
- Quantidade: 1 equipamento Cisco modelo 3745 em São Paulo
- Desembalagem;
- Ligação e teste;
- Montagem dos módulos;
- Configuração (SNMP, IP, VLANs, roteamento);
- Testes operacionais

Critério de Conclusão

Esta instalação estará concluida quando houver comunicação na rede LAN através das portas GigabitEthernet e WAN entre o roteador na rede da ECT e uma rede conectada por meio das portas seriais V.35 e ATM E3. A configuração do Roteador deverá permitir que as estações de trabalho que estejam em perfeito funcionamento e com a configuração de endereçamento TCP/IP coerente com o determinado pelo projeto de endereçamento da rede possam realizar comunicação através do protocolo TCP/IP, o que será demonstrado pela execução de um comando PING de uma estação ao roteador da rede remota.

Instalação dos Roteadores Tipo 2 em Brasília

- Quantidade: 2 equipamentos Cisco modelo 1751 em Brasília

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 871
Doc.

- Desembalagem;
- Ligação e teste;
- Montagem dos módulos;
- Configuração (SNMP, IP, VLANs, roteamento);
- Testes operacionais

Critério de Conclusão

Esta instalação estará concluída quando os parâmetros da rede de homologação forem customizados nos roteadores e houver comunicação entre as redes via interfaces de LAN(10/100 FastEthernet) e seriais V.35. Para as interfaces de voz analógicas deverão ser fornecidos os parâmetros para a devida configuração como dial-peers, gateways e numero de ramal local.

Implementação da Solução do Servidor de Segurança Lógica Tipo 01

- Quantidade: 4 Firewalls Cisco Firewall PIX 535 em Brasília
- Quantidade: 4 Firewalls Cisco Firewall PIX 535 em São Paulo

Atividades a serem realizadas:

- Instalação dos firewalls Cisco Pix;
- Configuração de endereços e máscaras;
- Configuração de rotas
- Configuração de interfaces
- Definição dos objetos da rede
- Configuração do log e dos filtros de registros
- Configuração do log de eventos
- Configuração de NAT (se necessário)
- Configuração de alta disponibilidade
- Testes de funcionalidade

Critério de Conclusão

Esta etapa estará concluida quando da verificação das funcionalidades e políticas de segurança estabelecidas no firewall através de um teste de conexão permitida (por exemplo: SMTP) e um teste de conexão não autorizada (por exemplo: ICMP).

1002
ECT/2005 - CN
CPMI - CORREIOS
Fls. Nº 3675
Pág. 35
Doc. 3608

verificação será efetuada através da análise do arquivo de log dos firewalls. Além disso, será realizada a verificação da redundância de configuração, quando ao se interromper o funcionamento do firewall principal (simulando uma queda de energia), o firewall de backup (failover) deverá assumir suas funcionalidades.

Implementação da Solução do Servidor de Segurança Lógica Tipo 02

- Quantidade: 2 Firewalls Cisco Firewall PIX 525 em Brasília
- Quantidade: 2 Firewalls Cisco Firewall PIX 525 em São Paulo

Atividades a serem realizadas:

- Instalação dos firewalls Cisco Pix;
- Configuração de endereços e máscaras;
- Configuração de rotas
- Configuração de interfaces
- Definição dos objetos da rede
- Configuração do log e dos filtros de registros
- Configuração do log de eventos
- Configuração de NAT (se necessário)
- Configuração de alta disponibilidade
- Testes de funcionalidade

Critério de Conclusão

Esta etapa estará concluida quando da verificação das funcionalidades e políticas de segurança estabelecidas no firewall através de um teste de conexão permitida (por exemplo: SMTP) e um teste de conexão não autorizada (por exemplo: ICMP). A verificação será efetuada através da análise do arquivo de log dos firewalls. Além disso, será realizada a verificação da redundância de configuração, quando ao se interromper o funcionamento do firewall principal (simulando uma queda de energia), o firewall de backup (failover) deverá assumir suas funcionalidades.

Implementação da Solução de Sistema para Detecção de Intrusão

- Quantidade: 1 equipamento Cisco modelo IDS 4250 em Brasília
  Quantidade: 1 equipamento Cisco modelo IDS 4250 em São Paulo

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº
Doc.

- Instalação e configuração dos sensores Cisco em segmentos da rede a serem definidos na reunião de planejamento
- Configuração para identificar padrões de ataque no tráfego da rede
- Configuração para atualização automática dos padrões de ataque
- Configuração das condições de alerta e reações automáticas
- Testes de Funcionalidade

Critério de Conclusão

Verificação da funcionalidade dos produtos através da programação da detecção de um padrão conhecido, como a aplicação FTP para um determinado servidor. O sistema deverá detectar esta tentativa e alertar o administrador sobre a ocorrência através de um e-mail.

Implementação da Solução de Gerência de Firewall e IDS(VMS), Switches e Roteadores(CiscoWorks-LMS e CiscoWorks-RWAN) e Autenticação de usuários(ACS)

Software:

São Paulo:

1 x MC – Management Center para Firewall(FW-MC);

1 x MC - Management Center para IDS (IDS-MC);

1 x CiscoWorks LMS para switches

1 x CiscoWorks RWAN para roteadores;

1 x Cisco Secure para autenticação;

Brasília:

1 x MC – Management Center para Firewall(FW-MC);

1 x MC - Management Center para IDS (IDS-MC);

1 x CiscoWorks LMS para switches

1 x CiscoWorks RWAN para roteadores;

1 x Cisco Secure para autenticação;

- Instalação dos últimos patches e correções no Windows NT Server
- Instalação e configuração do FW-MC para firewall

CPMI - CORREIOS
Fls Nº 877
Doc. 3698

- Instalação e configuração do IDS-MC para IDS
- Instalação e configuração do LMS
- Instalação e configuração do RWAN;
- Instalação e configuração do ACS;
- Definição dos objetos e da topologia da rede no MC- Management Center.
- Configuração das políticas de segurança nos firewalls dos clusters e as políticas de detecção do IDS
- Testes de funcionalidade

Critério de Conclusão

Visualização e configuração através das consoles de gerência dos firewalls, switches, IDS, concentrador de VPN e de usuário.

2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager

Estes serviços baseiam-se no seguinte escopo de serviço:

Site Brasília/DF - BSB

SERVIDOR INTEL TIPO 1 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 14 (catorze) Servidores.

SERVIDOR INTEL TIPO 2 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 29 (vinte e nove) Servidores.

CPMI - CORREIOS
Fls Nº 878
Doc. 3698

Itautec

SERVIDOR INTEL TIPO 3 - Instalação e Configuração Windows 2000 Server ou Windows Server 2003 Standard Edition em 27 (vinte e sete) Servidores.

Site São Paulo/SP - SPM

SERVIDOR INTEL TIPO 1 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 7 (sete) Servidores.

SERVIDOR INTEL TIPO 2 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 6 (seis) Servidores.

SERVIDOR INTEL TIPO 3 - Instalação e Configuração Windows 2000 Server ou Windows Server 2003 Standard Edition em 24 (vinte e quatro) Servidores.

Esta solução prevê a instalação e configuração dos servidores relacionados nesta proposta de serviço, nas localidades de Brasília/DF e São Paulo/SP, sendo estes os únicos sites para realização do serviço.

COMPONENTES DE SERVIÇOS PROFISSIONAIS

Os serviços profissionais, dentro das premissas estabelecidas, estão traduzidos através das atividades abaixo:

- Etapa E01 - Planejamento
- Etapa E02 - Instalação e Configuração do ambiente Plataforma Windows 2000/2003.
- Etapa E03 - Instalação e Configuração de MS Cluster Service
- Etapa E04 - Instalação e Configuração do SAN Manager
- Etapa E05 - Finalização

A seguir, apresentamos a descrição detalhada das etapas. Qualquer alteração no escopo do Projeto, conforme previsto no Edital do Pregão No. 050/2003 – CPL/AC da ECT, será avaliada para verificação de possíveis alterações na alocação de recursos e na duração das etapas.

Etapa E01 - Planejamento

Descrição

Reunião entre a ITAUTEC e a ECT que endereçará os pontos relevantes para realização dos serviços.

RQS nº 03/2005 - CN CORREIOS
Pág. 39
Fls. Nº
Doc.

Itautec

Atividades a Desenvolver

- Levantar informações detalhadas para a execução das atividades técnicas destes serviços.
- Levantamento de pré-requisitos de HW e SW.
- Definir procedimentos e datas para a execução destes serviços.
- Apresentar a arquitetura da solução para a ECT e suas compatibilidades no ambiente a ser implementado.
- Definir o processo de instalação, para o ambiente de Cluster e SAN que estarão envolvidos nesta proposta de serviço.

Critério de Conclusão

Esta etapa estará concluída quando as informações sobre o sistema da ECT forem registradas, todos os pré-requisitos necessários à execução destes serviços forem analisados e quando os procedimentos, processos e datas tiverem sido acordados entre a ITAUTEC e a ECT.

Etapa E02 - Instalação e Configuração do ambiente Plataforma Windows 2000/2003, para adequação a arquitetura de rede

Fase 1 - Instalação e Configuração

Descrição

Nesta etapa estaremos instalando e configurando o ambiente plataforma Windows 2000/2003, assim disponibilizando esta arquitetura para os sites Brasília/DF e São Paulo/SP, consistindo esta instalação e configuração em seu ambiente LAN.

Site Brasília/DF - BSB

SERVIDOR INTEL TIPO 1 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 14 (catorze) Servidores.

SERVIDOR INTEL TIPO 2 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 29 (vinte e nove) Servidores.

SERVIDOR INTEL TIPO 3 - Instalação e Configuração Windows 2000 Server ou Windows Server 2003 Standard Edition em 27 (vinte e sete) Servidores.

RQS nº 03/2005 - CN
CORREIOS
Pág. 40
Fls. Nº 880
Doc. 3668

Itautec

Site São Paulo/SP - SPM

SERVIDOR INTEL TIPO 1 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 7 (sete) Servidores.

SERVIDOR INTEL TIPO 2 - Instalação e Configuração Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition em 6 (seis) Servidores.

SERVIDOR INTEL TIPO 3 - Instalação e Configuração Windows 2000 Server ou Windows Server 2003 Standard Edition em 24 (vinte e quatro) Servidores.

Pré-Requisitos

- A estrutura de telecomunicação disponibilizada.
- O acesso à rede corporativa disponibilizada.
- A ECT deve fornecer e disponibilizar a estrutura de endereçamentos TCP/IP, classe, máscaras, segmentos e todas as informações chaves para estes serviços que consiste o ambiente de rede da ECT.

Atividades a Desenvolver

- Instalação e configuração do sistema operacional Plataforma Windows 2000/2003 nos servidores INTEL.
- Instalação no ambiente Plataforma Windows 2000/2003, o último nível de service pack e fixes.
- Configuração de sistemas de arquivos (partições e drive lógicos, definição de diretórios).
- Customização de relação de confiança entre domínios conforme solução disponibilizada pelo cliente em seu ambiente de rede.
- Configuração de protocolos de comunicação, definições de endereçamentos e nomes, adotados pelo cliente em seu ambiente de rede.
- Definição e customização dos serviços básicos da Plataforma Windows 2000/2003.
- Definição de DHCP Server, DNS Server, WINS Server, solicitados pelo cliente em seu ambiente de rede e disponibilizado pela ECT.
- Instalação e configuração dos devices drives, conforme os dispositivos existentes no servidor (placas de rede, discos).
- Arquitetura na Plataforma Windows 2000/2003 na segurança de usuários, monitoramento de acessos, em 1 (um) servidor Domain Controller.

Critério de conclusão

CPML - CORREIOS
Fls Nº 881
Doc.

Itautec

Esta etapa estará encerrada quando a arquitetura na Plataforma Windows 2000/2003 nos servidores envolvidos nestes serviços estiverem em funcionalidade de comunicação; e o administrador esteja efetuando logon em seu domain controller.

Fase 2 - Estrutura da Plataforma Windows 2000/2003

Descrição

Nesta fase estaremos construindo a arquitetura do ambiente na Plataforma Windows 2000/2003, com configurações, gerência e processos.

Atividade a desenvolver

- Configuração da estrutura de rede, protocolo TCP/IP em ambiente LAN.
- Configuração do ambiente de gerência de comunicação nos servidores INTEL do ambiente de rede na Plataforma Windows 2000/2003 nos sites Brasília /DF e São Paulo/SP envolvidos no escopo desta proposta.
- Estrutura de domínio, trust e segmento de rede, segundo informações disponibilizadas pela ECT.

Critério de conclusão

Esta etapa estará encerrada quando os Servidores INTEL estiverem em funcionalidade de comunicação na plataforma Windows 2000/2003 no ambiente LAN, processando com êxito um acesso a outro servidor na plataforma Windows 2000/2003, através do Server Manager da plataforma Windows 2000/2003, sendo que estes acessos são em protocolo TCP/IP já instalado e em perfeita funcionalidade na ECT.

Etapa E03 - Implementação MS Cluster Service

Fase 1 - Planejamento para a estrutura do Cluster

Descrição

Nesta etapa estaremos procedendo a reuniões de planejamento, focando estes serviços no detalhamento de informações, documentação sobre a melhor disponibilização do ambiente.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 882
Doc.

Atividades a Desenvolver

- Levantamento dos dados sobre a estrutura física do ambiente dos servidores.
- Detalhes sobre ambiente de rede, protocolos, serviços e acessórios de rede.
- Informações sobre os servidores a serem clusterizados, sobre os serviços genéricos, aplicativos, banco de dados, sistema operacional e outras informações que sejam relevantes a estes serviços.
- Detalhes dos técnicos do ECT referente aos servidores envolvidos nestes serviços.
- Documentação desde planejamento e disponibilização do mesmo.

Critério de conclusão

Esta fase estará concluída quando as dúvidas e informações forem coletadas e for executado um levantamento de informações do ambiente a ser clusterizado e servidores.

Fase 2 - Instalação e Configuração do MS SQL 2000 Server Enterprise Edition em ambiente de MS Cluster Service

Descrição

Nesta etapa estaremos instalando e configurando o ambiente MS Cluster Service para o SGBD MS SQL 2000 Server Enterprise Edition, assim disponibilizando esta arquitetura nas 02 (duas) localidades abaixo:

Site Brasília/DF - BSB

SERVIDOR INTEL TIPO 1- Instalação do MS SQL 2000 Server Enterprise Edition em 05 (cinco) Servidores e instalação e configuração MS Cluster Service em 05 (cinco) Servidores.

Site São Paulo/SP - SPM

SERVIDOR INTEL TIPO 1 - Instalação do MS SQL 2000 Server Enterprise Edition em 02 (dois) Servidores e instalação e configuração MS Cluster Service em 02 (dois) Servidores.

Pré-Requisitos

- A estrutura física totalmente disponibilizada.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Nº 883
Doc. 3698

- O acesso aos servidores a serem "clusterizados" disponíveis.

Atividades a Desenvolver

- Instalação do MS SQL 2000 Server Enterprise Edition para disponibilidade de arquitetura.
- Instalação do Microsoft Cluster Service para disponibilidade de arquitetura.
- Instalação dos níveis de service pack e fixes definidos pelo cliente.
- Configuração de sistemas de arquivos (partições e drive lógicos, definição de diretórios).
- Definição e customização de serviços de MS Cluster Service
- Instalação e configuração dos devices drives.
- Configuração dos respectivos subsistemas de discos externos, conexão destes ao servidor do cluster e instalação dos devices drivers.
- Implementação da arquitetura MS Cluster Service em 07 (sete) servidores.

Critério de conclusão

Esta fase estará concluída quando a arquitetura MS Cluster Service entre 07 (sete) servidores, estiver em comunicação com o node manager e visualizando o node client no servidor de administrador do MS Cluster Service.

Fase 3 - Estrutura da arquitetura do ambiente Cluster Service

Descrição

Nesta fase estaremos construindo a arquitetura do ambiente cluster service, com configurações, gerência e processos.

Atividade a desenvolver

- Estrutura do Node Manager, integrando todos os membros ou grupos do cluster service
- Configuração da estrutura do Database Manager, repositório das configurações do cluster service
- Gerência de recursos e failover, assinalando os recursos e grupos de decisões e apropriadas ações para o cluster service

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 881
Doc. 3698

- Estrutura do processamento de eventos, conectando os componentes de serviço de cluster, operações e controle dos serviços de cluster de inicialização.
- Configuração do ambiente de gerência de comunicação, com os nodes do serviço de cluster.

Critério de conclusão

Esta fase estará concluída quando o Node Manager estiver em 03 (três) grupos de cluster service criado no node manager, e o database manager estiver sido instalado para armazenagem das informações do cluster server.

Fase 4 - Estrutura de monitoramento de recursos do cluster service

Descrição

Neste processo estaremos ativando o monitoramento de mensagens do ambiente de serviço de cluster.

Atividades a Desenvolver

- Configuração de gerenciamento de processo e comunicação com o serviço de cluster, através do Remote Procedure Call (RPC).
- Monitoramento em até 07 (sete) Nodes dentro do serviço de cluster.

Critério de conclusão

Esta fase estará concluída quando a comunicação através de mensagens dentro do ambiente de cluster estiver sido efetuada entre o node manager e o node client, e possa ser visualizada uma mensagem na console administrador no node manager.

Fase 5 - Estrutura da base para o serviço de cluster

Descrição

Nestes processos estaremos implementando a base para o serviço de cluster e configuração de ambiente.

Atividade a desenvolver

- Estrutura de discos físicos para o ambiente desta etapa do Projeto.

RQS nº 03/2005 - CN CORREIOS
Pág. 45
Fls Nº
Doc.

- Criação de volumes lógicos dentro da arquitetura dos servidores e cluster.
- Definição de arquivos e diretórios.
- Adequação dos endereços TCP/IP e nomes na rede corporativa.
- Controle dos serviços e aplicativos.

Critério de conclusão

Esta fase estará concluída quando todas as configurações físicas (discos) e lógicas (volumes) estiverem sido visualizadas na console de administrador do node manager.

Fase 6 - Estrutura essencial da arquitetura do serviço de cluster

Descrição

Nesta etapa estaremos finalizando a estrutura do cluster server, com as configurações essenciais para a implementação do serviço de cluster.

Atividades a Desenvolver

- Instalação e configuração do Node Manager em até 07 (sete) Servidores Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition.
- Configuração do Database Manager em até 07 (sete) Servidores Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition.
- Configuração do Resource Manager/Failover Manager em até 07 (sete) Servidores Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition.
- Instalação e configuração de uma interface de administrador em até 07 (sete) Servidores Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition.

Critério de conclusão

Esta fase estará concluída quando for executado com sucesso, a conexão entre 07 (sete) Servidores e a comunicação dos Node Managers com os Nodes Clients configurados na arquitetura do serviço de cluster, através da visualização dos grupos de cluster nos node managers.

Etapa E04 - Instalação e Configuração do ambiente SAN Manager

RQS nº 03/2005 - CN
Pad. 46
CPMI - CORREIOS
Fls. Nº 880
Doc.

Itautec

Fase 1 - Instalação e Configuração

Descrição

Nesta etapa estaremos instalando e configurando o ambiente SAN Manager, assim disponibilizando esta arquitetura para o site Brasília/DF e site São Paulo/SP, consistindo esta instalação e configuração em seu ambiente SAN.

Site Brasília/DF – BSB

SERVIDOR ADICIONAL - Instalação e configuração do SAN Manager Server/Console em 1 (um) Servidor Windows 2000 Server ou Windows Server 2003 Standard Edition em ambiente SAN.

SERVIDOR INTEL TIPO 1 - Instalação e configuração do SAN Manager Agent em 14 (catorze) Servidores.

SERVIDOR INTEL TIPO 2 - Instalação e configuração do SAN Manager Agent em 29 (vinte e nove) Servidores.

Site São Paulo/SP - SPM

SERVIDOR ADICIONAL - Instalação e Configuração do SAN Manager Server/Console em 1 (um) Servidor Windows 2000 Server ou Windows Server 2003 Standard Edition em ambiente SAN.

SERVIDOR INTEL TIPO 1 - Instalação e configuração do SAN Manager Agent em 7 (sete) Servidores.

SERVIDOR INTEL TIPO 2 - Instalação e configuração do SAN Manager Agent em 6 (seis) Servidores.

Pré-Requisitos

- O acesso a SAN corporativa disponibilizada.
- A estrutura física e lógica do ambiente SAN da ECT.

Atividades a Desenvolver

- Instalação e configuração do SAN Manager Server na plataforma Windows 2000 Server ou Windows Server 2003 Standard Edition.
- Instalação e configuração do SAN Manager Console na plataforma Windows 2000 Server ou Windows Server 2003 Standard Edition.
- Configuração dos SAN Manager Agents
- Definição de customização do SAN Manager Server/Console.
- Configuração do SAN Manager Server/Console em ambiente SAN.

RQS nº 03/2005 - CN
SRM/CORREIOS
Pág. 47
Fls: Nº 0881
Doc. 3698

- Definição e customização em até 05 (cinco) eventos do SAN Manager em sua console.
- Configuração de Auto Discovery para os objetos relacionados na SAN.

Critério de conclusão

Esta etapa estará encerrada quando a arquitetura SAN Manager Server/Console nos servidores envolvidos nesta etapa do projeto estiver em funcionalidade de comunicação com a SAN, visualizando os objetos relacionados na SAN no escopo desta etapa do projeto.

Etapa E05 - Finalização

Descrição

Reunião entre a ITAUTEC e a ECT para encerramento desta etapa do projeto, o que marca o final do dos serviços referentes à Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager.

Atividades a Desenvolver

- Executar o software MS SYSTEM STRESS da MICROSOFT pelo período de 72 (setenta e duas) horas ininterruptas em cada equipamento;
- Executar reunião de encerramento desta etapa do Projeto;
- Recolher o Termo de Conclusão de Serviços Profissionais.

Critério de Conclusão

Esta etapa do Projeto estará finalizada após a reunião de encerramento e a assinatura do Termo de Conclusão de Serviços Profissionais.

2.5 Serviço de Implementação de Ambiente pSeries Regatta, Storage e Backup

RQS nº 03/2005 - CN
CORREIOS
Pág. 48
Fls. Nº 886
Doc.

Etapa E01 - Alocação de Recursos

Descrição

Este período será o de mobilização que é necessário para que ITAUTEC e Cliente possam garantir os pré-requisitos necessários abaixo para o início do Projeto.

Pré-requisitos

- Alocação de profissionais pela ITAUTEC e Cliente para cada um dos seguintes papéis:
  - ✓ Gerente de Projeto (ITAUTEC): Ponto Focal da ITAUTEC em relação aos contatos com o Cliente, referentes a este Projeto;
  - ✓ Gerente de Projeto (ECT): Ponto Focal para toda e qualquer comunicação com a ITAUTEC relativa a este serviço e que terá autoridade para decidir em nome do cliente nas questões relativas a este projeto, ou escalar o assunto dentro da ECT.
  - ✓ Especialistas (ITAUTEC): execução das atividades escopo desta proposta;
  - ✓ Analistas Técnicos (ECT): acompanhar a instalação do ambiente e apto a responder ao questionamento do profissional ITAUTEC em relação à execução dos serviços que dependem de definições adotadas pelo Cliente.

Etapa E02 - Reunião de Planejamento

Descrição

Reunião entre a ITAUTEC e o Cliente que endereçará os pontos relevantes para execução do Serviço de Implementação do Ambiente pSeries Regatta, com definição e montagem do cronograma de trabalho.

Atividades a Desenvolver

Reunião entre ITAUTEC e ECT para :

- Levantar informações detalhadas para a execução das atividades técnicas desta etapa do Projeto;
- Endereçar os pontos relevantes para a execução desta etapa do Projeto;
- Verificação da disponibilidade de requisitos de HW e SW para a execução desta etapa do Projeto;
- Definir procedimentos, roteiros, datas e responsabilidades para a execução desta etapa do Projeto;
- Confecção e validação do cronograma de trabalho.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 889
Doc. 3628

Itautec

Ao final desta reunião, o Gerente de Projeto do Cliente deve definir os pontos focais a serem alocados para cada uma das etapas. Desta forma, ao final desta etapa, os Gerentes de Projeto da ITAUTEC e ECT estarão de posse de um cronograma de trabalho detalhado e validado. Este será utilizado para acompanhamento e controle do andamento desta etapa do Projeto.

Pré-requisitos

- Alocação do Gerente de Projeto da ITAUTEC/Cliente;
- Confirmação de data, local e recursos necessários para a reunião.

Responsabilidades

- ITAUTEC: preparação e condução da reunião;
- ECT: alocação das facilidades necessárias para a reunião e estruturação da agenda de trabalho com pontos focais do cliente.

Critério de Conclusão

Esta etapa estará concluída quando os procedimentos, roteiros, datas e responsabilidades, além do próprio cronograma de trabalho, tiverem sido acordadas entre a ITAUTEC e ECT.

Local

Nas instalações do cliente.

Etapa E03 - Implementação AIX e Configuração de Regatta (LPAR)

Atividades a Desenvolver

O serviço ITAUTEC de Implementação de AIX coloca um Especialista de Serviços à disposição nas instalações do Cliente para coordenar a instalação de 11 (onze) equipamentos pSeries Regatta, instalar e configurar o Sistema Operacional AIX e configurar as partições LPAR, de acordo com a quantidade definida no desenho da solução proposta para cada equipamento Regatta em cada uma das localidades, São Paulo e Brasília.

Serão implementados também 4 (quatro) equipamentos pSeries, considerando instalação e configuração do AIX, sendo 2(dois) em cada localidade de São Paulo e Brasília para atuarem como servidores de Backup ITSM.

RQS nº 03/2005 - CN - CORREIOS
Pág. 50
Fls. Nº
Doc.

Itautec

Este serviço também prevê transferência de conhecimentos básicos para o pessoal técnico do Cliente.

O Especialista de Serviços ITAUTEC irá executar as seguintes atividades em cada equipamento pSeries e pSeries Regatta a ser instalado:

- planejar, com o representante do Cliente, a instalação do novo equipamento pSeries;
- coletar, com o representante do Cliente, dados sobre o sistema e a configuração desejada;
- conectar 1 (uma) console IBM suportada e verificar a comunicação com a CPU pSeries;
- criar "file systems" padrão, "file systems" para os programas-produto IBM e selecionar uma interface padrão;
- instalar o sistema operacional AIX;
- configurar as Partições LPAR;
- definir um usuário no AIX, indicado pelo Cliente, com os parâmetros e senhas apropriados;
- configurar o ambiente de trabalho (desktop);
- configurar o TCP/IP;
- instalar e configurar Licenças do Compilador C;
- prover instrução básica, durante a execução dos serviços;
- realizar uma cópia de segurança (mksysb backup) do sistema instalado;
- criar e entregar um documento contendo a configuração do sistema.

Critérios de Conclusão

As responsabilidades da ITAUTEC estarão terminadas quando as atividades acima forem finalizadas e o servidor pSeries estiver pronto para que as aplicações e dados sejam instaladas pelo Cliente.

Isto ficará evidenciado quando puder ser efetuado um ping a partir do equipamento pSeries para um outro equipamento da rede local do cliente.

Etapa E04 - Implementação HACMP

Atividades a Desenvolver

Em resposta à demanda para alta disponibilidade nos servidores de aplicações comerciais, a ITAUTEC oferece o Serviço de Implementação de AIX HACMP. Este serviço, com

BOS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 891
Doc.

HACMP, pode aumentar potencialmente a disponibilidade de seus recursos computacionais ao permitir que um processador pSeries de reserva (backup) assuma os endereços de rede e recursos compartilhados de disco de um servidor com problemas. Após uma falha, os usuários podem acessar os recursos computacionais a partir do servidor de reserva, com mínima perda de continuidade.

Ao fornecer este serviço, a ITAUTEC assume a responsabilidade de conduzir a sessão de planejamento da instalação, a instalação do software, configuração, teste de falha, e instrução básica do uso e administração do HACMP.

Ao término do serviço, o software HACMP estará instalado e operacional para 14 (quatorze) clusters de 2 (dois) nós cada, na configuração HotStandy, Mutual Takeover ou Concurrent para o Site de Brasília e 6(seis) clusters com 2(dois) nós cada no site de São Paulo.

Também será efetuada a configuração do Software HACMP em dois clusters de 2 (dois) nós cada, sendo um em São Paulo e outro em Brasília, para os equipamentos pSeries que atuarão como Servidores de Backup ITSM

A ITAUTEC é responsável pelas seguintes atividades:

- **Planejamento da instalação**

Planejar a instalação do HACMP com seu representante. Os seguintes tópicos serão discutidos:

- ✓ Compatibilidade das aplicações com o HACMP
- ✓ Verificação dos requerimentos de hardware e software
- ✓ Planejamento da rede TCP/IP
- ✓ Planejamento da rede serial
- ✓ Planejamento dos discos compartilhados e componente LVM
- ✓ Planejamento do servidor de aplicações
- ✓ Planejamento do grupo de recursos
- ✓ Planejamento das máquinas-cliente
- ✓ Determinação de Pontos Únicos de Falha
- ✓ Notificação de falha em hardware redundante
- ✓ Planejamento de backup
- ✓ Determinação da necessidade de pessoal e recursos do Cliente
- ✓ Cronograma das atividades de instalação

- Instalação do HACMP - Instalar HACMP para AIX e correções (PTF) necessárias

RQS nº 03/2005 - CN CPMI - CORREIOS Fls: Nº 892 3698 Doc.

- Configuração do HACMP
  - ✓ Configurar rede
  - ✓ Configurar discos compartilhados
  - ✓ Configurar o servidor de aplicações HACMP com os korn shell script padrões que serão modificados para as aplicações do Cliente

- Notificação de Erros e Eventos

Configurar a notificação de erros e eventos para discos redundantes, adaptadores de rede e falhas no nó via e-mail para o usuário root.

- Teste de falha e recuperação

Demonstrar a recuperação para falhas em adaptadores de rede, disco e nó (crash de máquina).

- Registro de instalação (Documentação)

Fornecer um registro da instalação com informações sobre a configuração do HACMP.

- Instrução básica

Durante a execução deste serviço, profissionais designados pelo Cliente irão receber instrução básica sobre as atividades realizadas de instalação e administração do AIX e HACMP.

- Cópia de segurança (backup)

Um backup mksysb será iniciado após a implementação do HACMP.

Pré-Requisitos

- O cluster será limitado a 2 (dois) na configuração hot standby ou mutual takeover utilizando grupos de recursos em cascata ou rotativos;
- O IP Address Takeover (IPAT) será configurado para um endereço IP de serviço para o modo hot standby ou dois endereços para mutual takeover;
- A instalação e teste do HACMP requerem exclusividade do sistema, ou seja, o uso produtivo do sistema não deve ser programado durante serviços de instalação, configuração e teste do HACMP. É necessário acesso dedicado ao sistema durante a execução do serviço;
- Somente as aplicações que não requeiram intervenção manual após a queda do sistema, poderão ser automatizadas no HACMP.
- O Cliente deve :
  - ✓ Designar até dois administradores de sistema para estarem disponíveis durante a execução deste serviço, a fim de receberem a instrução básica;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 893
Doc:

- ✓ Assegurar que as pessoas responsáveis por este projeto, pelo banco de dados, pela rede, pelo sistema e aplicações participem da reunião de planejamento
- ✓ Fornecer acesso dedicado ao sistema para execução deste serviço;
- ✓ Fornecer as seguintes informações sobre seu ambiente:
  - a password 'root'
  - Características de localização e tamanho para os 'volume groups' de discos compartilhados, volumes lógicos e/ou filesystems para os dados da aplicação residindo em discos compartilhados
  - Múltiplos endereços de IP requeridos pelos pSeries
- ✓ Realizar cópias de segurança, caso o sistema já se apresente em produção (sistema operacional mais dados)

Critérios de Conclusão

A ITAUTEC terá completado sua participação neste projeto quando o processo de takeover terminar com sucesso, ou seja, quando, após o crash da máquina sevidora, a máquina backup assumir os recursos configurados pelo HACMP em todos os clusters.

Etapa E05 - Implementação do ITSM

Descrição dos Serviços

Esta proposta descreve as atividades do serviço de implementação da solução ITSM para o cliente ECT. Este serviço está dividido em 05 (cinco) fases, descritas a seguir, sendo que em todas elas haverá treinamento "on-the-job" ao cliente.

Atividades a Desenvolver

Fase 1 - Apresentação de conceitos básicos do ITSM

O serviço iniciará com uma apresentação sobre os conceitos básicos do ITSM para o pessoal técnico do cliente, visando a participação ativa do cliente durante todo o serviço.

Esta fase estará concluída após esta apresentação técnica, que tem duração estimada entre 3 (três) e 8 (oito) horas, dependendo da participação do cliente.

Fase 2 - Instalação do servidor ITSM (plataforma AIX)

1- Instalação e configuração básica de 4 (quatro) ITSM Servers em equipamentos com sistema operacional AIX, sendo 2 (dois) localizados em São Paulo e 2 (dois) em Brasília.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 054
Fls Nº 0901
Doc.

2- Instalação e configuração no AIX, e no ITSM de uma library 3584 e suas respectivas unidades de fita.

3- Testes de backup e restore do servidor ITSM na library instalada anteriormente.

4- Instalação do ITSM SysBack em 15 (quinze) equipamentos pSeries.

Esta fase estará concluída quando for possível fazer um backup de teste do próprio servidor na biblioteca de fitas via ITSM.

Fase 3 - Instalação dos clientes ITSM nas plataformas AIX e Windows

1- Instalação e configuração do ITSM Client em 134 (cento e trinta e quatro) equipamentos com sistema operacional AIX ou Windows, considerando ITSM Clients for SAN e ITSM Clients for LAN.

2- Testes de backup e restore de cada um dos clients no servidor ITSM instalado na fase 2.

Esta fase estará concluída quando for possível fazer um backup de teste (de pequeno volume) de cada um dos clients no servidor ITSM instalado na fase 2.

Fase 4 - Instalação do ITSM for Database (Oracle)

1- Instalação e configuração do TDP for Oracle em 11 (onze) equipamentos.

2- Testes de backup e restore (de pequeno volume) de cada um dos servidores de Dados oracle no servidor ITSM instalado na fase 2 através do TDP for Oracle.

Esta fase estará concluída quando for possível fazer um backup de teste (de pequeno volume) de cada um dos Servidores Oracle no servidor ITSM instalado na fase 2 através do TDP for Oracle.

Fase 5 - Instalação do ITSM for Database (SQL)

1- Instalação e configuração do TDP for MSSQL em 7 (sete) equipamentos.

2- Testes de backup e restore (de pequeno volume) de cada um dos Servidores de Dados MSSQL no servidor ITSM instalado na fase 2 através do TDP for MSSQL.

Esta fase estará concluída quando for possível fazer um backup de teste (de pequeno volume) de cada um dos Servidores MSSQL no servidor ITSM instalado na fase 2 através do TDP for MSSQL.

Fase 6 - Instalação do ITSM for Mail (Exchange)

1- Instalação e configuração do TDP for MSExchange em 8 (oito) equipamentos.

RQS nº 03/2005 - CN
CORREIOS
Pág. 55
Fls Nº 895
Doc.

2- Testes de backup e restore (de pequeno volume) de cada um dos Servidores MSExchange no servidor ITSM instalado na fase 2 através do TDP for MSExchange.

Esta fase estará concluída quando for possível fazer um backup de teste (de pequeno volume) de cada um dos servidores MSExchange no servidor ITSM instalado na fase 2 através do TDP for MSExchange.

Fase 7 - Customização inicial do ambiente ITSM do Cliente

Com base nas necessidades do cliente, a ITAUTEC fará a customização inicial do ambiente, com o objetivo de deixar as funções do ITSM disponíveis ao término do serviço.

O cliente terá participação ativa na definição dos objetivos desta etapa, porém, algumas tarefas básicas serão executadas pela ITAUTEC, descritas a seguir:

1- Inicialização das fitas para o uso do ITSM;

2- Criação das políticas de backup;

3- Criação de schedules;

4- Definição de storage pools;

5- Definição do mecanismo de backup do servidor ITSM.

Esta fase estará concluída quando o teste de backup e restore de acordo com a política de backup definida ocorrer com sucesso.

Etapa E06 - Implementação do Sistema de Cofre para Ambiente ITSM

Atividades a Desenvolver

- Levantamento da quantidade de dados a serem copiados para o Cofre
- Definição das janelas de tempo entre as operações de cópia e retirada das fitas
- Implementação dos Copy Storage Pools
- Implementação das operações de check-in e check-out das fitas a serem transportadas entre o site e o cofre.
- Definição dos procedimentos de Restore do ITSM DB e Storage Pools em caso de desastre com os volumes do site.
- Teste de Restore de Volumes dos Copy Storage Pools

Critério de Conclusão

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 806
Doc.

Esta Etapa estará concluída quando o restore dos volumes de copy storage pool tiver sido concluído com sucesso e todos os processos do sistema de cofre tenham sido automatizados.

Etapa E07 - Implementação da Storage Area Network (SAN)

Descrição

O serviço contemplado nesta etapa tem como objetivo a implementação de 06 (seis) Switches 2109 para a Configuração da Rede SAN.

Fase 1 - Planejamento

Descrição

Reunião entre a ITAUTEC e a ECT que endereçará os pontos relevantes para execução desta etapa.

Atividades a Desenvolver

- Levantar informações detalhadas para execução das atividades técnicas desta etapa.
- Análise do atendimento dos requisitos básicos para esta etapa.
- Definir procedimentos e datas para a execução desta etapa.
- Definir plano de testes para validação desta etapa.

Critério de Conclusão

Esta Etapa estará concluída quando as informações sobre o sistema do Cliente forem registradas; quando houver a confirmação de todos os pré-requisitos necessários à execução desta etapa e quando os procedimentos e datas forem acordados entre a ITAUTEC e a ECT.

Fase 2 - Distribuição Lógica dos Switches

Descrição

Esta etapa tem como objetivo fazer a distribuição lógica das portas dos switches da rede SAN.

Atividades a Desenvolver

ROS nº 03/2005 - CN
CPMI CORREIOS
Pág. 57
Fls. Nº 897
Doc.

- Planejar a distribuição das portas;
- Realizar a configuração nos switches.

Critério de Conclusão

Esta etapa estará concluída quando os switches 2109 estiverem configurados e disponíveis.

Fase 3 - Tape Pooling

Descrição

Esta etapa tem como objetivo conectar os drives da LTO 3584 na rede SAN.

Atividades a Desenvolver

- Configurar o gateway;
- Conectar os drives.

Critério de Conclusão

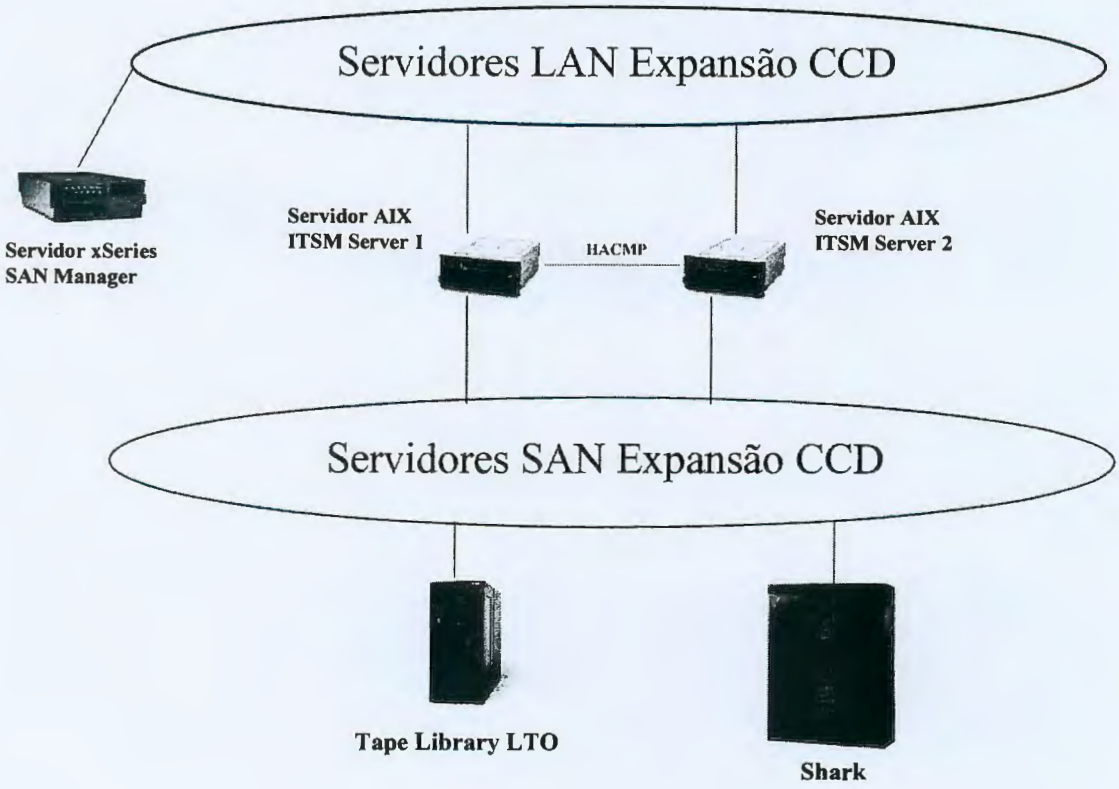
Esta Etapa estará concluída quando os drives da LTO estiverem sendo acessados pelos servidores da rede SAN através dos switches.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc.

Itautec

2.5.1 Ilustração da Solução

Correios BSB - Arquitetura Proposta – Expansão CCD

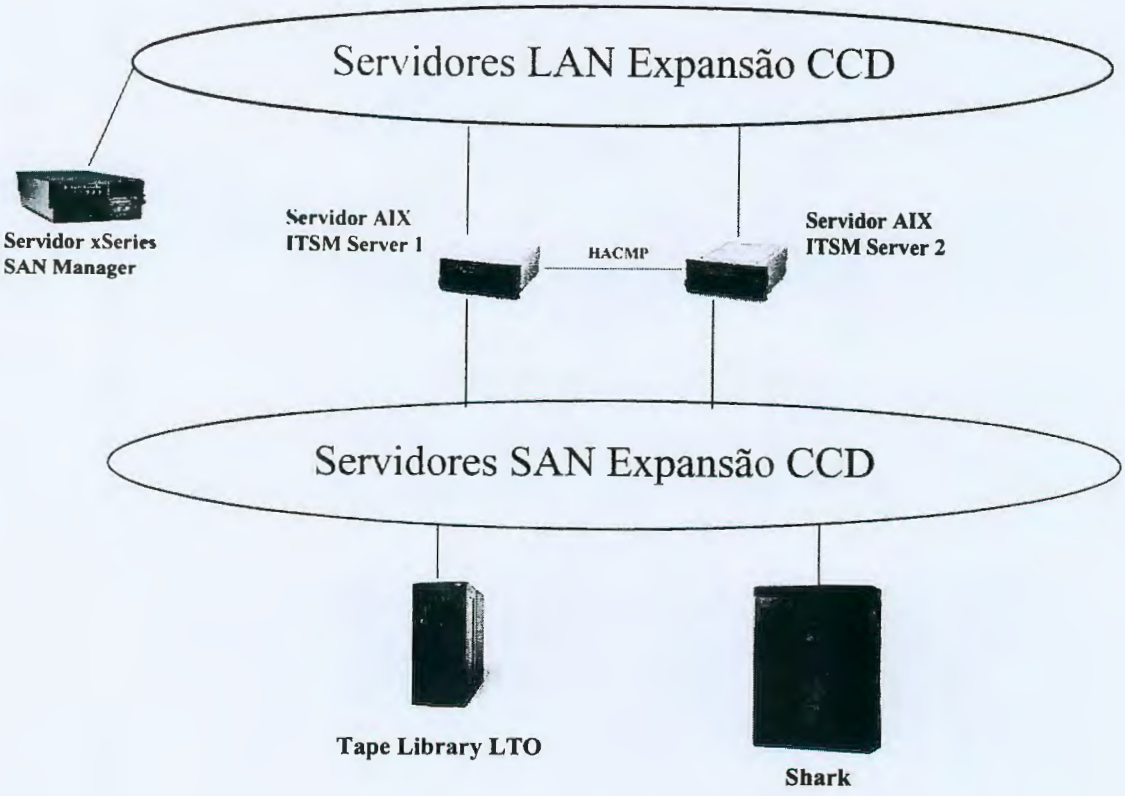


RQS nº 03/2005 - CN
EPM - CORREIOS
Fls Nº 899
Doc.

Itautec

9998

Correios SP - Arquitetura Proposta – Expansão CCD



RQS nº 03/2005 - CN
Pag. 60 CORREIOS
Fls. Nº 900
Doc.

Itautec

2.6 Implementação do IBM Director

Descrição dos Serviços

O serviço compreenderá a instalação e Configuração de 1 IBM Director Server em São Paulo para atender 43 Clients, e 1 IBM Director Server em Brasília para atender 76 clientes. Para tal, estaremos seguindo as seguintes atividades:

- Planejamento em São Paulo e Brasília
- Instalação do Server em São Paulo e Brasília
- Instalação dos Clients em São Paulo e Brasília
- Testes e Ajustes em São Paulo e Brasília
- Documentação para São Paulo e Brasília

Planejamento

Atividades a Desenvolver:

- Identificar com absoluta clareza o ambiente do cliente, registrando as informações em ata de reunião.
- Definir o Cronograma de Atividades

Instalação do Server

Atividades a Desenvolver:

- coletar, com o representante do Cliente, dados sobre o sistema e a configuração desejada;
- implementação de contingência e falha de discos nos servidores conforme adotado pelo cliente na fase de planejamento, com as configurações RAID1 ou RAID5, caso aplicável;
- instalação do sistema operacional Windows 2000 Server ou Windows Server 2003 Standard Edition em 02 (dois) servidores;
- instalação no ambiente Windows 2000/2003 Server do último nível de Service Pack e fixes em até 02 (dois) servidores;
- configuração de sistemas de arquivos (partições e drives lógicos, definição de diretórios);
- customização de relação de confiança entre domínios conforme solução adotada pelo cliente na fase de planejamento;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 61
Fls. Nº 961
Doc.

- configuração de protocolos de comunicação, definições de endereçamentos e nomes, adotada na fase de planejamento;
- definição e customização dos serviços básicos do Windows 2000/2003 Server;
- instalação e configuração dos devices drives, conforme os dispositivos existentes no servidor (placas de rede, discos);
- montar a estrutura do Windows 2000/2003 Server, configurando os serviços e grupos de acesso a volumes;
- configuração da estrutura de rede, protocolo, LAN e WAN;
- montar a estrutura de domínio, trust e segmento de rede;
- Instalação do IBM Server Director baseado em informações obtidas no planejamento.
- Executar o software MS SYSTEM STRESS da MICROSOFT pelo período de 72 (setenta e duas) horas ininterruptas em cada equipamento.

Pré-requisitos do Cliente:

- A estrutura de telecomunicação disponibilizada;
- O acesso a rede corporativa disponibilizada;
- Fornecimento da estrutura de endereçamentos TCP/IP disponibilizados, classe, máscaras, segmentos e todas as informações chaves para o projeto.

Nota:

- Algumas das atividades acima podem não ser executadas, dependendo do tipo de configuração proposta e do ambiente de rede Windows 2000/2003 Server já existente no Cliente.
- O critério de conclusão para Instalação do Server será quando a arquitetura Windows 2000/2003 Server de 02 (dois) servidores estiverem configuradas compartilhando diretórios.

Instalação dos Clients

Atividades a Desenvolver:

- Instalação dos Clientes do IBM Server Director em 119 Clients distribuídos entre São Paulo e Brasília.

Testes e Ajustes

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 902
Doc.

Atividades a Desenvolver:

- Realizar testes e ajustes no produto para garantir o perfeito funcionamento do sistema.

Workshop

A ITAUTEC realizará um Workshop em Brasília e um Workshop em São Paulo, a fim de esclarecer a operação dos softwares de gerenciamento em questão.

Documentação

Atividades a Desenvolver:

- Criar um documento refletindo as atividades realizadas em termos de instalação e customização do Produto IBM Director na ECT.

Nota:

- É recomendável que pelo menos 02 (dois) recursos da ECT, por localidade, acompanhem as atividades de Instalação e Customização do IBM Director.
- A funcionalidade de gerenciamento de pré-falha é disponibilizado através da implementação de um sistema de gerenciamento baseado no IBM Director, que intercepta os sinais de PFA (Predective Failure Analisys) gerados por componentes/opcionais que suportam esta capacidade, tais como CPU, VRM (voltage regulator module), discos, ventiladores e fontes de alimentação.

2.7 Implementação do gerenciamento eHealth Enhanced Sysedge

Atividades

Instalação, licenciamento e configuração dos softwares Concord nos 119 servidores Intel e nas 92 partições AIX (RISC).

Os agentes e suas extensões, serão instalados, licenciados e configurados para monitorar os "File System" do servidor gerenciado, os respectivos serviços e aplicações, além de

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 963
Doc.

enviar estas informações para o ambiente HP OpenView e Concord eHealth atual dos Correios.

Quando especificado pelos Correios, os seguintes itens serão configurados para que sejam gerenciados nos servidores e no ambiente eHealth dos Correios:

- Serviços de configuração dos agentes Enhanced Sysedge a fim de medir o tempo de resposta dos serviços DNS, HTTP, HTTPS, SMTP, POP3, FTP ou TCP dos servidores.
- Serviços de configuração dos agentes Enhanced Sysedge para monitorar o desempenho e falhas das aplicações Exchange, Oracle, MS SQL, Apache ou IIS

Integração do ambiente operacional ao ambiente de gerenciamento dos Correios

1. Concord eHealth

A ITAUTEC realizará a descoberta e agendamento de relatórios para os seguintes elementos no Concord e Health dos Correios referentes à licitação:

- Agentes SystemEdge dos servidores

Serão criadas regras no Live Health para a monitoração de elementos e o envio de alarmes para o ambiente HP Openview.

1.1 HP Openview NNM

Será criado um mapa no HP Openview NNM com todos os elementos do ambiente em questão.

1.2 HP Openview OVO

Dentro do funcionamento do HP Openview OVO serão realizadas as seguintes alterações nas estruturas para se adequar os novos elementos desse projeto ao ambiente já utilizado:

- Criação de usuários
- Criação de grupos de usuários

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 64
Fls Nº 904
3698
Doc.

Itautec

- Adição de nodes
- Configuração de grupos de nodes
- Modificação da console de alarmes

ECT - 03/2005 - CN
CORREIOS
Fls Nº 905
Doc.

Itautec

2.8 Treinamento Oficial

Sistemas Operacionais Microsoft (MCSA)

Descrição	Código	Duração (dias)	Horas
Managing a Microsoft Windows Server 2003 Environment	2274	5	40
Maintaining a Microsoft Windows Server 2003 Environment	2275	3	24
Updating Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows Server 2003	2208	5	40
Implementing a Microsoft Windows Server 2003 Network Infraestructure: Network Hosts	2276	2	16
Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infraestructure: Network Services	2277	5	40
Implementing and Supporting Microsoft Windows XP Professional	2272	5	40
Installing, Configuring, and Administering Microsoft Windows XP Professional	2285	3	24
Microsoft Windows 2000 Networking and Operating System Essentials	2151	3	24
Deploying and Supporting Microsoft Management Server 2.0	828	5	40
Administering Microsoft System Management Server 2.0	827	3	24
Deploying and Managing Microsoft Internet Security and Aceleration Server 2000	2159	3	24

160 horas-aula por aluno
03 Turmas de 06 alunos em Brasília
01 Turma de 06 alunos em São Paulo

pSeries & AIX-RS/6000

AIX Para Usuários Finais

Descrição	Código	Duração (dias)	Horas
AIX Básico Ver.5L	Q1313BR	5	40

RQS nº 03/2005 - CN
EPMI - CORREIOS
Fls. Nº 906
Doc.

Itautec

Administração do Sistema AIX

Descrição	Código	Duração (dias)	Horas
AIX Ver. 5L Administração de Sistema AIX I: Implementação	Q1314XBR	5	40
AIX Ver. 5L Administração de Sistema AIX II: Determinação de Problemas	Q1316BR	5	40
AIX Ver. 5L Administração de Sistema AIX III: Administração de Desempenho	Q1318BR	5	40
AIX V5L Administração de Sistema IV: Gerência de Armazenamento	Q1320BR	4	32
AIX Ver. 5L Administração de Sistema V: Work Load Manager	Q1319BR	3	24
AIX Ver. 5L Jumpstart para Profissionais UNIX	Q1818BR	4	32
AIX Ver. 5L Diferenças da Implementação	Q1237BR	3	24
pSeries Logical Partitioning para AIX 5L	Q1370BR	5	40

Segurança AIX

Descrição	Código	Duração (dias)	Horas
Segurança em AIX I : Mecanismos Baseados em Host	Q1341BR	3	24
Segurança em AIX II: Mecanismos de Rede	Q1342BR	2	16
Segurança em AIX III: Mecanismos de Internet	Q1343BR	3	24

Programação AIX

Descrição	Código	Duração (dias)	Horas
Introdução a Programação em Linguagem C	Q1070BR	4,5	36
Programação RS/6000 Korn Shell	Q1123BR	5	40
Programação RS/6000 PERL V	Q1122BR	3	24
AIX Ver. 5L Ambiente de Programação de Aplicações	Q1325BR	5	40
Workshop: Migrando de Solaris para AIX Ver. 5L	Q1329BR	4	32
Programação PERL para Sistemas Abertos em World Wide Web	Q1124BR	5	40

Comunicação AIX

Descrição	Código	Duração (dias)	Horas
AIX Ver. 5L Configuração TCP/IP	Q1307BR	5	40
AIX Ver. 5L Network Installation Management (NIM)	Q1308BR	2	16

AIX High Availability

Descrição	Código	Duração (dias)	Horas
Administração de Sistema HACMP I: Planejamento e Implementação	Q1554BR	5	40

RQS nº 03/2005 - C
CPMI - CORREIO
Fls. Nº 907
Doc.

Itautec

eServer Cluster 1600

Descrição	Código	Duração (dias)	Horas
eServer Cluster 1600 Administração do Sistema I: Implementação	Q1991BR	5	40
eServer Cluster 1600 Administração do Sistema II: Usando PSSP	Q1996BR	5	40

Linux

Descrição	Código	Duração (dias)	Horas
Fundamentos de Linux e Instalação	QLX02BR	5	40
Administração de Sistema Linux I: Implementação	QLX03BR	5	40
Linux Jumpstart para Administradores de Sistemas UNIX	QLX15BR	4	32
Administração de Sistema Linux II: Segurança de Host	QLX41BR	3	24
Administração de Rede Linux I: TCP/IP e TCP/IP Services	QLX07BR	5	40
Administração de Rede Linux II: Segurança de Rede e Firewalls	QLX24BR	5	40
Linux e-business com Apache	QLX25BR	3	24
Integrando Linux com Windows (Samba)	QLX26BR	2	16
Programação Perl para Linux e World Wide Web	QLX28BR	5	40

160 horas-aula por aluno
03 Turmas de 06 alunos em Brasília
01 Turma de 06 alunos em São Paulo

MS SQL Server 2000

Descrição	Código	Duração (dias)	Horas
Administering a MS SQL Server 2000 Database	2072	5	40
Programing a MS SQL Server 2000 Database	2073	5	40

80 horas-aula por aluno
02 Turmas de 06 alunos em Brasília

Segurança Lógica

Segurança

Descrição	Código	Duração (Dias)	Horas
Secure Cisco Networks	SECUR	5	40
Cisco Secure Pix Firewall Advanced (CSPFA)	CSPFA	5	40
Cisco Secure Virtual Private Network (CSVPN)	CSVPN	4	32
Cisco Secure Intrusion Detection System (CSIDS)	CSIDS	3	24
Cisco Safe Implementation (CSI)	CSI	4	32

160 horas-aula por aluno
02 Turmas de 06 alunos em Brasília ou São Paulo ou Rio de Janeiro

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 008
Doc.

Itautec

Cisco Product Training

Routing & Switching

Descrição	Código	Duração (Dias)	Horas
Interconnecting Cisco Network Devices (ICND)	ICND	5	40
Building Scalable Cisco Internetworks (BSCI)	BSCI	5	40
Building Cisco Multilayer Switching Networks (BCMSN)	BCMSN	5	40
Building Cisco Remote Access Networks (BCRAN)	BCRAN	5	40
Cisco Internetwork Troubleshooting (CIT)	CIT	5	40
TCP/IP com enfoque LAN/WAN	TCP/IP - LAN	5	40

220 horas-aula por aluno

02 Turmas de 06 alunos em Brasília

01 Turma de 06 alunos em São Paulo

Tivoli System Management

Tivoli Performance and Availability

Descrição	Código	Duração (Dias)	Horas
Tivoli Distributed Monitoring 4.1	TM220BR	2	16
IBM Tivoli Monitoring 5.1	TM230BR	2	16
IBM Tivoli Enterprise Console 3.8	TM120BR	3	24
Programming Rules for the Tivoli Enterprise Console 3.8	TM210BR	2	16
Tivoli Decision Support 2.1 for Implementors	TZ050BR	2	16
Tivoli NetView for UNIX 7.1 for Administrators	TV070BR	5	40
Tivoli NetView for NT for Administrators	TV060BR	5	40
IBM Tivoli Business Systems Manager 2.1 Fundamentals	TM030BR	2	16
IBM Tivoli Service Level Advisor 1.2 Workshop	TM572BR	2	16
IBM Tivoli Web Site Analyzer 4.2	TM270BR	2	16

Tivoli Configuration Mgmt. & Operations

Descrição	Código	Duração (Dias)	Horas
Tivoli Infrastructure 4.1	TM160BR	3	24
Tivoli Infrastructure 4.1 for Senior Administrators	TM260BR	4	32
Novo! IBM Tivoli Configuration Manager 4.2	TM170BR	5	40
Tivoli Software Distribution 4.1	TM145BR	4	32
Tivoli Inventory 4.0	TM200BR	2	16
Tivoli Workload Scheduler 8.1 Scheduling and Operations	TW050BR	3	24
Tivoli Workload Scheduler 8.1 Administration	TW040BR	2	16

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 999
Doc.

SCS Q. 01 Bloco "F" 11º Andar – Ed. Camargo Corrêa -- Brasília-DF CEP: 70397-900 - Fone: (61) 323-3031 Fax: (61) 226-1251

Itautec

Tivoli Storage Management

Descrição	Código.	Duração (Dias)	Horas
Tivoli Storage Manager Implementation 5.1	TS570BR	5	40
Tivoli Storage Manager 5.1 Enhancements, Tuning and Troubleshooting	TS580BR	4	32
Tivoli Disaster Recovery Manager 5.1Implementation	TS590BR	2	16

Tivoli Security

Descrição	Código.	Duração (Dias)	Horas
IBM Tivoli Risk Manager Installation & Administration	TR020BR	2	16
IBM Tivoli Access Manager for e-business 3.9 System Administration	TR390BR	5	40
IBM Tivoli Access Manager for Business Integration 4.1 System Administration	TR440BR	3	24
IBM Directory Server 4.1 Administration	TR360BR	3	24

OS/390 Solutions

Descrição	Código.	Duração (Dias)	Horas
IBM Tivoli Workload Scheduler 8.1 for z/OS Scheduler's Workshop	TM400BR	4	32
IBM Tivoli Workload Scheduler 8.1 for z/OS Implementation	TM410BR	5	40

80 horas-aula por aluno

02 Turmas de 06 alunos em Brasília

01 Turma de 06 alunos em São Paulo

CPMI CORREIOS
Fls Nº 910
Doc.

Itautec

Plataforma INTEL - MCSA - Microsoft Certified System Administrator - 12 vagas

- Exame 70-290 - Managing and Maintaining a Microsoft Windows Server 2003 Environment
- Exame 70-291 - Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infraestructure
- Exame 70-270 - Installing, Configuring and Administering Microsoft Windows XP Professional
- Exame 70-210 - Installing, Configuring and Administering Microsoft Windows 2000 Professional
- Exame 70-086 - Implementing and Supporting Microsoft Systems Management Server 2.0
- Exame 70-227 - Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition
- Exame 70-228 - Installing, Configuring and Administering Microsoft SQL Server 2000 Enterprise Edition

Plataforma RISC - IBM 191 - IBM Certified Specialist - pSeries AIX System Administration - 12 vagas

Conectividade - 12 vagas

- 640-607 CCNA
- 642-801 BSCI
- 643-811 BCMSN
- 642-821 BCRAN
- 643-831 CIT

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 71
Fls. Nº 911
Doc.

Itautec

3. Pauta de Distribuição e Especificações Técnicas dos Equipamentos

3.1 Pauta de Distribuição

Os equipamentos que compõe a presente Proposta serão distribuídos entre Brasília e São Paulo, segundo o quadro abaixo:

DISTRIBUIÇÃO DOS RECURSOS			
TIPO DE EQUIPAMENTO	**CCD AC (BRASÍLIA)**	**CCD SPM (SÃO PAULO)**	**TOTAL**
SERVIDOR INTEL TIPO 01	14	7	21
SERVIDOR INTEL TIPO 02	29	6	35
SERVIDOR INTEL TIPO 03	27	24	51
SERVIDOR RISC TIPO 01	8	3	11
SWITCH TIPO 1	2	2	4
SWITCH TIPO 02	4	2	6
SWITCH TIPO 03	4	2	2
SWITCH TIPO 04	8*	4*	12*
SWITCH TIPO 05	1	1	2
ROTEADOR TIPO 01	1	1	2
ROTEADOR TIPO 02	2	0	2
UNIDADE DE BACKUP ROBOTIZADO	1	1	2
SERVIDOR DE SEGURANÇA LÓGICA TIPO 01	2	2	4
SERVIDOR DE SEGURANÇA LÓGICA TIPO 02	1	1	2
SERVIDOR PARA DETECÇÃO DE INTRUSÃO	1	1	2
TOTAL			**162**

* dependendo da configuração fornecida

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 912
Doc.

Itautec

REQUISITOS ESSENCIAIS AOS EQUIPAMENTOS OBRIGATÓRIOS

2. ASPECTOS GERAIS

Os itens descritos a seguir serão observados para todos os produtos que compõem a proposta técnica.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
2.1 – Comprovação de Performance para os Equipamentos da plataforma RISC	• Estão sendo ofertados equipamentos IBM pSeries p690 Turbo com 16 CPUS de 1.7 GHz. Este equipamento foi auditado pelo Standard Performance Corporation com 32 CPUs. Está sendo apresentada a comprovação por documentação adequada do valor de SPECjbb2000 auditado pelo Standard Performance Evaluation Corporation – SPEC (www.spec.org) para o equipamento cotado. • O equipamento cotado não foi auditado com o número de processadores proposto, desta forma estamos informando um cálculo estimado. O valor utilizado para estimativa de SPECjbb2000 foi obtido em	• 16.740 specjbb	Sim	Manual 25 SPECjbb2000 IBM Corporation IBM eServer pSeries 690 Turbo (págs. 1 e 2) Manual 18 Cálculo para comprovação de Performance (Equipamentos RISC) (pág. 1)

RQS nº 03/2005 CN CPMI - CORREIOS
Fls. Nº 0143
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	equipamento auditado, com o mesmo tipo/série e tipo de CPU (modelo, clock e cache), do equipamento cotado, o que será comprovado por documentação adequada de auditoria. • A performance estimada, foi calculada com base na fórmula:SPECjbb2000 estimado = SPECjbb2000 auditado * (nº de CPU ofertadas / nº CPU auditada) • O benchmark de SPECjbb2000 utilizado é superior ao valor máximo especificado.			
2.2 – Comprovação de Performance para os Equipamentos da plataforma INTEL	• Todos os equipamentos INTEL para os quais foram solicitados valor de performance baseado em tpm-C, possuem documentação comprobatória adequada do valor do tpm-C auditado pelo Transaction Processing Performance Council – TPC		Sim	**Tipo 01 : Manual 26** Pag. 05 http://www.tpc.org/results/individual_results/IBM/ibm.x440-8way.c5.1.es.030404.pdf **Tipo 02 : Manual 26**

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 0911 Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	(www.tpc.org) para o equipamento cotado ou para equivalente, conforme documentação em anexo. • Para o servidor Intel Tipo 3 foi utilixzada a formula de performance estimada abaixo:Tpm-C estimado = tpm-C auditado * (no. De CPU ofertadas / no. CPU auditada)			Pag. 21 http://www.tpc.org/results/individual_results/IBM/ibm.x360_2.0GHz.c5.1.es.03022801.pdf **Tipo 03 : Manual 26** Pag.37 http://www.tpc.org/results/individual_results/IBM/ibm.x235.c5.1.es.03071001.pdf
2.3 – Requisitos Gerais	• Os equipamentos serão novos de fábrica e entregues acondicionados adequadamente em caixas fechadas, de forma a permitir completa segurança durante o transporte; • Serão fornecidos pela ITAUTEC, quando da entrega e instalação dos produtos, todos os cabos, acessórios, manuais e documentações completas, que são necessários ao pleno funcionamento dos equipamentos, softwares e		Sim	

RQS nº 03/2005 - CP
CPMI - CORREIOS
Fls. Nº 0176
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	periféricos; • Não serão consideradas para efeitos de somatório das quantidades mínimas exigidas, controladoras Fibre Channel e de Rede integradas na placa de sistema; • Serão aceitas, para efeito de somatório, Placas de Rede Ethernet com até 2 (duas) interfaces por placa, na montagem da configuração dos Servidores RISC Tipo 01; • A ECT solicitará o remanejamento de módulos de switch, interfaces de rede ou fibre channel entre os servidores fornecidos, a qualquer momento da vigência do Contrato, sem ônus adicionais.			
2.4 – Garantia	• É de total responsabilidade da ITAUTEC, a garantia do pleno funcionamento e operabilidade dos produtos fornecidos, durante a vigência do		Sim	

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0948
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	Contrato.			
2.5 – Alimentação Elétrica	• Todos os equipamentos Intel destinados ao CCD de Brasília operam em 220 (duzentos e vinte) volts. • Todos os equipamentos Intel destinados ao CCD de São Paulo operam em 220 (duzentos e vinte) volt, e através da instalação de equipamentos adicionais que realizam compatibilidade elétrica, conforme especificado no subitem 1.3.1.alínea "i" do ANEXO 1-A, estaremos atendendo este item.		Sim	Manual 26 Tipo 01 - Pag. 03 Tipo 02 – Pag. 19 Tipo 03 – Pag. 35 Página da Web do componente : - Fonte de Alimentação: Tipo 02 – P/N: 31P6108 – Pag. 27-29 Tipo 03 – Pag. 45
2.6 – Assistência técnica	• A ITAUTEC prestará os serviços assistência técnica nos locais de instalação dos equipamentos, nas cidades de Brasília/DF e São Paulo/SP; • Os serviços prestados devem englobar a substituição de peças e componentes defeituosos dos equipamentos,		Sim	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	bem como a depuração e resolução de problemas relacionados ao AMBIENTE OPERACIONAL fornecido pela ITAUTEC.			
2.7 – Recursos Mínimos de Particionamento para os Servidores RISC	• O Equipamento RISC Tipo 01 está sendo ofertado com, no mínimo, 8 (oito) partições físicas ou lógicas e são expansíveis a 16 (dezesseis) partições físicas ou lógicas. • O número especificado de partições é alcançado com a simples configuração de software fornecido para este fim, sem a necessidade de adição de nenhum hardware ou software adicionais. Estão sendo ofertadas 2 (duas) consoles em cada localidade, sendo que todas as consoles gerenciam todos os equipamentos em cada localidade; • As partições funcionarão de modo que cada uma execute [illegible]	• O Equipamento RISC tipo 01 ofertado é expansível a 32 partições físicas ou lógicas.	Sim	Declaração Comprobatória. Manual 24, página2 Declaração Comprobatória. Declaração Comprobatória.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	sua própria imagem de sistema operacional e que a falha do sistema operacional de uma partição não interfira, em hipótese alguma, no funcionamento das demais partições; • Os equipamentos RISC Tipo 01 permitirão o remanejamento de recursos de CPU, Memória e I/O entre as partições; • Os equipamentos RISC Tipo 01 serão fornecidos com todos os recursos de hardware e software necessários à criação do número mínimo de partições especificadas para cada equipamento; • A ITAUTEC fornecerá notebooks, com no mínimo: Processador INTEL Pentium IV 2,0 GHz, 256MB de memória RAM, Placa de Rede e Placa de Faxmodem, para desempenhar a função de			Manual 24, pág 2 Manual 34: Página 1

RQS nº 03/2005 CN CPMI - CORREIOS
Fls Nº 0210
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	gerenciamento e suporte remoto dos servidores RISC. Fornecerão 4 (quatro) notebooks para o CCD de Brasília e 1 (um) notebook para o CCD de São Paulo.			
2.8 – Recursos Mínimos de Gerenciamento do Hardware requeridos para os Servidores INTEL	▪ Todos os servidores Intel fornecidos, inclusive os adicionais, possuem mecanismos de detecção de pré-falhas para os componentes vitais ao sistema : CPU, Memória e Discos; ▪ Através da instalação e implementação de um servidor adicional com o sw IBM Director, seus agentes e console de gerenciamento estará disponibilizada a gerência de pré-falhas, sendo disponibilizado um ambiente para cada localidade (CCD de Brasília e CCD de São Paulo)	Adicionalmente, os servidores Intel Tipo 01, 02 , 03 e Adicionais suportam gerenciamento de pré-falha para as fontes de alimentação, ventiladores.	Sim	Manual 26 Tipo 01 - Pag. 03 Tipo 02 – Pag. 19 Tipo 03 – Pag. 35 • A funcionalidade de gerenciamento de pré-falha é disponibilizado através da implementação de um sistema de gerenciamento baseado no IBM Director, que intercepta os sinais de PFA (Predective Failure Analisys) gerados por componentes/opciona

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0170
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
				is que suportam esta capacidade, tais como CPU, VRM (voltage regulator module), CPU, discos, ventiladores e fontes de alimentação.
2.9 – Recursos Mínimos de hardware e software para os Servidores INTEL	Todos os servidores INTEL ofertados adicionalmente, serão montados em RACK de 19", conforme o subitem 7, a serem fornecidos pela ITAUTEC; Os equipamentos Intel adicionais serão fornecidos com os seguintes recursos : • Sistema Operacional Microsoft Windows Server 2003 Standard Edition, instalado, licenciado e configurado para Rede Corporativa dos Correios;		Sim	Manual 26: Página da Web do Rack P/N 9306-420 / 9306-421 - Pag. 65-68 O Sistema Operacional Microsoft Windows Server 2003 Enterprise Edition a ser licenciado é conforme endereço internet http://www.microsoft.com/catalog/display.asp?subid=22&site=11261, e será instalado e configurado conforme

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0121
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
				"Etapa E02 - Instalação e Configuração do ambiente Plataforma Windows 2000/2003" do item "2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager", conforme página 38.
	• 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios;			O Agente SysEdge a ser licenciado é conforme Manual 35 - endereço internet http://www.concord.com, e será instalado e configurado conforme item "2.7 - Implementação do gerenciamento eHealth Enhanced Sysedge,

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls Nº 0122
Doc. 3698

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
				conforme página 63.
	• 1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios;			Manual 36: IBM Tivoli Storage Manager for AIX Administrator's Guide, pag. 3
	Estamos ofertando como servidores adicionais, equipamentos idênticos aos configurados para Intel Tipo 02 e 03. Todos os servidores adicionais possuem os seguintes componentes de hw :			Manual 37: "IBM Tivoli Storage Manager for Windows – Quick Start" Pag. 1
	• Fontes de alimentação instaladas na configuração máxima do equipamento com recurso de troca sem interrupção (Hot Swap/Hot			Manual 26: Servidores Adicionais 01 = Intel Tipo 03

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0295
Doc. 3602

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	plug) e alimentação elétrica em 220V para as duas localidades, com frequência 60 (sessenta) Hertz; • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 02 (dois) circuitos, o equipamento conitunará funcionando sem prejuízo às aplicações. • Interfaces de rede padrão Ethernet PCI 10/100/1000 BaseT em conformidade com os padrões IEEE 802.3ab e 802.3u com possibilidade de gerenciamento SNMP;			Manual 26: Fonte de Alimentação Pag. 35, 43-45 Manual 26: P/N: 31P6301 Pag. 59-62 Manual 26: Servidores Adicioanais 02 = Intel Tipo 02 Manual 26: P/N : 31P6108 Pag. 19, 27-31 Manual 26: P/N : 31P6301

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0241
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	• As interfaces de rede conectarão os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.			Pag. 59-62 Proposta Econômica – item 1.3.1 pág 8
2.10 – Recursos Mínimos de hardware e software para os servidores RISC adicionais	• Os servidores Risc oferecidos adicionalmente serão montados em RACKS de 19". Os Racks serão fornecidos pela ITAUTEC. • A ITAUTEC está fornecendo e irá instalar e configurar, para todos os servidores RISC cotados adicionalmente os seguintes softwares: • Sistema Operacional AIX 64Bits, será instalado e configurado para Rede dos Correios, e está sendo proposto com número ilimitado de usuários simultâneos; • Sistema de Arquivos JFS		Sim	Manual 36 IBM Tivoli Storage Manager for AIX – Administrator Guide pág.3 Manual 24 5765-E62 IBM (pág. 1) Manual 24 5765-E62 IBM (pág. 2)

RQS nº 03/2005 CN CPMI – CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	• Ferramenta que permita o backup e restore do sistema operacional (Image Backup)			Manual 24 5765-E62 IBM (pág. 2) (pág. 3)
	• 1 licença do agente "Concord SystemEdge", devidamente instalado e configurado conforme orientação da equipe técnica dos Correios.			O Agente SysEdge a ser licenciado é conforme Manual 35 - endereço internet http://www.concord.com, e será instalado e configurado conforme item "2.7 - Implementação do gerenciamento eHealth Enhanced Sysedge, conforme página 63.
	• 1 licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos correios.			Manual 41: IBM Tivoli Storage Manager for AIX Quick Start, página 1.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0200
Doc.

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	• A ITAUTEC está fornecendo e irá instalar, para todos os servidores RISC cotados adicionalmente, os seguintes componentes de hardware: • Fontes instaladas na configuração máxima do equipamento, com recurso de troca sem interrupção (HotSwappable/HotPluggable) e alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5, freqüência de 60 (sessenta)Hertz; • As fontes de alimentação propostas são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2(dois) circuitos, o equipamento continue a			Manual 42: IBM Tivoli Storage Manager for System backup and Recovery Installation and User´s Guide, pág. vii Manual 21: 7028-6C4 IBM eServer pSeries 630 Model 6C4 (págs. 26 e 89) Manual 21 7028-6C4 IBM eServer pSeries 630 Model 6C4 (págs. 80 e 81) Manual 17

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0931
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	funcionar sem prejuízo das aplicações; • As interfaces de rede serão padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u com possibilidade de gerenciamento SNMP; • As interfaces de rede irão conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ45; ▪ 1 (uma) unidade de fita DDS4 interna. Está sendo prevista a entrega de 10 (dez) fitas DDS 3 e 2 (duas) fitas para limpeza.			Installation and Using Guide (pág. 1) Manual 19 IBM AIX 5L Operating System (pág. 3) Manual 21 7028-6C4 IBM eServer pSeries 630 Model 6C4 (pág. 84)
2.11 – Comprovação	• No fornecimento da documentação técnica é		Sim	

RQS nº 03/2005 - CN
CPMI - CORREIOS
FIS. Nº 0283
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
dos Requisitos Exigidos	documentação técnica, é exigido que sejam fornecidos obrigatoriamente todos os informes, conforme descritos nos subitens que seguem: ▪ A documentação que acompanha o equipamento deve ser em língua portuguesa, espanhola ou inglesa, preferencialmente em língua portuguesa; ▪ A identificação do Fabricante, da Marca e do Modelo do produto. • Comprovação, conforme MODELO VIII do ANEXO 3, de todos os atributos exigidos nesta planilha de Especificações, atestada pelo fornecimento do descrito em qualquer dos subitens que seguem ou pelo conjunto destes: • Prospecto técnico do modelo cotado, o qual deve ser preferencialmente no original ou fotocópia legível e			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	completa, com grifo nas características técnicas a serem informadas; ▪ Cópia legível e atual da página Internet do Fabricante onde constem às especificações técnicas do modelo do produto cotado, com grifo nas características técnicas a serem informadas			
2.12 – Organização da Documentação	• A ITAUTEC organizará toda a documentação dos equipamentos e softwares de forma que estejam reunidas e catalogadas, nos CCDs de Brasília e São Paulo, cópias da documentação técnica de cada tipo de equipamento ofertado, bem como cópias do CDs de instalação de cada software fornecido pela ITAUTEC; • A ITAUTEC entregará, sem ônus para a ECT , os CDs com toda atualização dos softwares fornecidos, durante a vigência do Contrato. Será entregue 1	A ITAUTEC estará fornecendo 02 (dois) conjuntos de cópias contemplando 01 (um) CD de instalação do Sistema Operacional Microsoft Windows Server 2003 Standard Edition, 01 (um) CD de instalação do Sistema Operacional Microsoft Windows 2000 Server, 01 (um) CD de instalação do Sistema Operacional Microsoft Windows Server 2003 Enterprise Edition, 01	Sim	

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 0990
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	(uma) cópia no CCD de Brasília e 1 (uma) cópia no CCD de São Paulo.	(um) CD de instalação do Sistema Operacional Microsoft Windows 2000 Advanced Server, 01 (um) CD de Microsoft SQL Server 2000 Enterprise Edition, sendo que 01 (um) conjunto será entregue no CCD de Brasília e 01 (um) conjunto será entregue no CCD de São Paulo.		
2.13 – Suporte Remoto	• A ITAUTEC disponibilizará todos os PRODUTOS necessários à implementação de uma estrutura de acesso remoto que permita a ITAUTEC acesso a rede corporativa da ECT , utilizando o Switch Tipo 5 a ser fornecido de acordo com o subitem 3.5.; • Esta estrutura de acesso remoto que será utilizado pela ITAUTEC possa prestar serviço de suporte remoto nas		Sim	

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 0091
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	• Situações em que a ECT julgue necessária. A estrutura de acesso remoto seguirá estritamente as Normas de Segurança definidas pela ECT.			
2.14 – Configuração das Ferramentas de Gerenciamento	• Durante o Treinamento de Gerenciamento, descrito no Subitem 1.9.2.3. do ANEXO 1-A, a ITAUTEC irá instalar e configurar os novos agentes 'Concord SystemEdge', integrando conforme os padrões da plataforma de Gerência já existente da ECT ; • A ITAUTEC configurará os agentes 'Concord SystemEdge' para, entre outras coisas, medir o tempo de resposta dos serviços de infra-estrutura, não se limitando a: DNS, HTTP, HTTPS, SMTP, POP3, FTP e TCP; • A ITAUTEC configurará os agentes 'ConcordSystemEdge' para que monitore o desempenho e falhas das		Sim	Conforme item "2.7 - Implementação do gerenciamento eHealth Enhanced Sysedge, conforme página 63 da Proposta Econômica Manual eHealth Service Response User Guide (Arquivo svcrsp.pdf), página 11. Obs: Service Availability é o novo nome comercial para o Service Response;

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0199
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim / Não)	Página da documentação Técnica
	aplicações Exchange, Oracle, MS SQL, APACHE e IIS; • A ITAUTEC habilitará o agente SNMP dos Roteadores, Switches e servidores fornecidos, conforme os padrões da ECT ; • A ITAUTEC configurará as ferramentas de gerenciamento existentes na ECT , não se limitando a: ▪ Integração de eventos no HP OpenView Operations; ▪ Criação e integração de regras inteligentes do Concord Live Health para envio de eventos ao HP OpenView Operations; ▪ Criação e geração de relatórios do Concord eHealth.			Manuais: ADVANTEDGE FOR MICROSOFT® EXCHANGE User Guide (Arquivo ExchangeUser.pdf), página 1-1; eHealth AIM for Oracle User Guide (Arquivo OracleUser.pdf), página 11; ADVANTEDGE FOR MICROSOFT SQL SERVER User Guide (Arquivo SQLUser.pdf), página 1-1; eHealth AIM for Apache User Guide (Arquivo ApacheUser.pdf), página 12; ADVANTEDGETM FOR MICROSOFT® IIS User Guide (Arquivo IISUser.pdf), página 1-1.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0999
Doc.

3. CONECTIVIDADE DA REDE

3.1. SWITCH TIPO 1 (LAYER-3 GE)

MARCA: CISCO

MODELO: CATALYST 6513

FABRICANTE: CISCO

OBJETIVO
Prover a conectividade dos equipamentos do CCD

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento(Sim / Não)**	**Página da documentação Técnica**
1 – Características Físicas	• Serão do tipo chassis.		Sim	• Pág. 1 – Switch_Tipo1_doc1
2 – Gabinete	• Chassis para ser instalado em RACK de 19" a ser fornecido juntamente com o equipamento. Virá acompanhado de kit de suporte específico para montagem em RACK de 19" com todos os módulos de interface, fontes de alimentação e ventiladores do tipo HOT-SWAPPABLE/HOT-PLUGGABLE.		Sim	• pág. 21 – Switch_Tipo1_doc1 • Pag. 2 – Switch_Tipo1_doc5
	• Disponibilizará de, pelo menos, 16		Sim	• pág. 25 –

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 3602
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
3 – Portas Gigabit-Ethernet	interfaces Gigabit Ethernet no padrão 1000BASE-SX , compatíveis com o padrão IEEE 802.3z; disponibilizará de, pelo menos, 192 portas 10/100/1000BASE-T, autosensing, compatíveis com o padrão IEEE 802.3ab, para cabos UTP Categoria 6 e conectores RJ-45; • Suportará a inclusão futura de, no mínimo, mais 48 portas 10/100/1000BASE-T.			Switch_Tipo1_doc1 Pag. 20 – Switch_Tipo1_doc7 Vide configuração na pág. 206 e 216 1 módulo com 16 portas 1000BaseSx e 4 módulos com 48 portas 10/100/1000Base-T com conectores RJ-45. • O chassis fornecido possui 3 slots livres permitindo até 144 portas 10/100/1000BaseT
4 – Hot-Swapping	• Será "HOT-SWAPPABLE/HOT-PLUGGABLE" em todos os módulos, permitindo as manobras de inserção/retirada de módulos sem interrupção do funcionamento dos demais.		Sim	• pág. 10 – Switch_Tipo1_doc1
5 – Balanceamento de carga	• Implementará balanceamento de servidores (tráfego) localizados em redes diferentes da rede deste		Sim	• Pag. 5 – Switch_Tipo1_doc9

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	SWITCH TIPO 01, baseado nos algoritmos Weighted Round Robin, Weighted Least Connections e URL Hashing; • Implementará balanceamento baseado em protocolos das camadas 4 a 7 (RM-OSI), incluindo TCP, UDP, FTP, DNS, SMT HTTP e IPSec; • Possuirá capacidade de vincular as conexões de cada cliente a um mesmo servidor por meio de endereçamento IP da fonte, de cookies e de Secure Socket Layer por identificador de sessão; • O balanceamento de tráfego possuirá redundância e alta disponibilidade com os outros SWITCHES do mesmo tipo, através dos protocolos HSRP ou VRRP, de maneira que, em caso de falha de um dos módulos de balanceamento, o estado de todas as conexões seja remanejado para o módulo redundante de forma totalmente transparente para os usuários;			Pag. 3 - Switch_Tipo1_doc9 • Pag. 4 – Switch Tipo1 doc10 e Pag. 2 – Switch Tipo1 doc12 • Pag. 3 – Switch_Tipo1_doc9 • Pag. 10 – Switch Tipo1 doc11

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 0296
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Será capaz de implementar adicionalmente qualidade de serviço (QoS) com diferenciação/priorização para todo o tráfego balanceado; • Suportará balanceamento global para servidores localizados em sites com diferentes saídas para a Internet.			• Pag. 3 – Switch_Tipo1_doc12 • Pag. 3 – Switch_Tipo1_doc12
7 – Gerenciamento	• Suportar as bases SNMP e MIB II, conforme RFC 1213, bem como os grupos RMON I (no mínimo quatro grupos) e todos os grupos RMON II.		Sim	• Pag. 11 – Switch_Tipo1_doc3
8 – Conectividade	• Permitirá no mínimo 8 (oito) grupos de agregação com, no mínimo, 8 (oito) enlaces cada, conforme padrão IEEE 802.3ad.		Sim	• Pag. 3 e 4 – Switch_Tipo1_doc6
9 – Roteamento	• Os SWITCHES fornecidos realizarão roteamento (camada 3).		Sim	• Pag. 3 - Switch_Tipo1_doc1
10 – QoS	• Os SWITCHES fornecidos implementarão no mínimo 4 (quatro) filas de prioridade em cada porta, permitirá a priorização do tráfego de rede e uma integração transparente de dados, voz e vídeo através do		Sim	• Pag. 14 – Switch_Tipo1_doc4 Pag. 2 – Switch_Tipo1_doc5

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	protocolo IEEE 802.1p com Cós (class-of-Service).			
11 – Fonte de Alimentação	• Fontes instaladas na configuração máxima do equipamento, com recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE) e alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação serão redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.		Sim	• Pag. 20 – Switch_Tipo1_doc1 Pag. A9 – Switch_Tipo1_doc7 • Pag. 20 – Switch_Tipo1_doc1
12 – Forwarding Performance	• Mínimo de 100 Mpps para Layer 2, Layer 3 e Layer 4.		Sim	• Pag. 4 – Switch_Tipo1_doc2
	• Implementará o protocolo STP (Spanning Tree Protocol) para cada VLAN configurada (uma sessão		Sim	• Pag. 25 – Switch_Tipo1_doc1

Doc. 3988
Fls. Nº 966
ECT - CORREIOS - SPMI
RCS nº 03/2005 - CN

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
13 – Gerais	VLAN configurada (uma sessão STP por grupo de portas); • Suportará múltiplos agrupamentos simultâneos de no mínimo 8 interfaces cada um em quaisquer interfaces de rede e em módulos diferentes de forma a agregar taxa de transmissão; • Possuirá a facilidade de trunking (IEEE 802.1Q) com outros switches; • Será capaz de implementar no mínimo 2 sessões simultâneas de espelhamento de tráfego, entrada e saída, de interfaces ou de VLANs; • Será fornecida ferramenta que permita o gerenciamento dos equipamentos e de todas as suas interfaces através de aplicação gráfica; • Serão fornecidos servidores adicionais para a instalação desta gerência.			• Pag. 2 – Switch_Tipo1_doc5 • Pag. 4 – Switch_Tipo1_doc1 • Pag. 6 – Switch_Tipo1_doc5 • Pag. 1 – Switch_Tipo2_doc13 • Proposta Econômica pág. 211 para Brasília e 221 para São Paulo.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0290
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica

3.2. SWITCH TIPO 2 (FE)

MARCA: CISCO

MODELO: CATALYST 2950G-48-EI

FABRICANTE: CISCO

OBJETIVO
Prover a conectividade dos equipamentos do CCD.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – Switch	• Será do tipo "stackable" (empilhável); • Permitirá empilhamento de no mínimo 6 (seis) unidades, por meio de links de no mínimo 1 Gbps		Sim	• Pag. 1 – Switch_Tipo2_doc1 • Pag. 12 – Switch_Tipo2_doc1 Pag. 2 –

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	redundantes, formando uma unidade gerenciável na rede através de um único endereço IP; • Os SWITCHES TIPO 2 serão montados em RACKS de 19"de acordo com o Subitem 7, a serem fornecidos pela IBM			Switch_Tipo2_doc1 Pag. 11 – Switch_Tipo2_doc1 • Pag. 8 – Switch_Tipo2_doc3
2 – Interfaces Fast e Gigabit Ethernet	• Possuirá o quantitativo mínimo de 48 portas com interfaces 10BaseT/100Base-TX, com detecção automática (switching fast ethernet autosense), full duplex, para cabos UTP Categoria 6 e conectores RJ-45 e, no mínimo, 1 portas "GBIC-based" Gigabit Ethernet, 1000BaseSX, e 1 porta disponível para empilhamento.		Sim	• Pag. 2 – Switch_Tipo2_doc2 Pag. 3 – Switch_Tipo2_doc2 Pag. 1 – Switch_Tipo2_doc6 Pag. 7 – Switch_Tipo2_doc7 Proposta Econômica pág. 8 "item 1.3.1"
3 – Gerais	• Possuirá sinalização visual de funcionamento e "status" das portas. • Será capaz de implementar espelhamento de tráfego de entrada e saída de interfaces ou de VLANs;		Sim	• Pag. 12 – Switch_Tipo2_doc2 • Pag. 10 – Switch_Tipo2_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 0411
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Gerenciável através de protocolo SNMP e possuirá suporte a MIB II, conforme RFC 1213, bem como Possui pelo menos 4 grupos RMON I; • Ser compatível com o padrão Ethernet IEEE 802.3u; • Implementará as normas IEEE 802.1Q e IEEE 802.1p; • Permitirá o controle de "broadcast storm"; • Suportará algum protocolo que permita limitar o flooding de tráfego IP multicast;			• Pag. 14 e 15 Switch_Tipo2_doc1 • Pag. 14 – Switch_Tipo2_doc1 Pag. 14 – Switch_Tipo2_doc1 • Pag. 7 – Switch_Tipo2_doc1 • Pag. 8 – Switch_Tipo2_doc1
3 – Gerais (Continuação)	• Implementará no mínimo 4 (quatro) filas de prioridade em cada porta, permitirá a priorização do tráfego de rede e uma integração transparente de dados, voz e vídeo através do protocolo IEEE 802.1p com CoS (class-of-Service);		Sim	• Pag. 4 – Switch_Tipo2_doc1

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0343
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Possuirá kits de fixação para instalação em RACKS de 19"e cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento; • Serão fornecidos todos os acessórios necessários à composição do empilhamento do switch, tais como cabos, conectores e interfaces; • Implementará, no mínimo, 200 VLANs no padrão IEEE 802.1Q, inclusive no empilhamento, isto é, permitirá o agrupamento em VLANs de portas de quaisquer switches da pilha; • Implementará o protocolo STP (Spanning Tree Protocol) para cada VLAN configurada (uma sessão STP por grupo de portas); • Possuirá barramento para empilhamento igual ou superior a 1 Gbps; • Será fornecida ferramentas que permitam o gerenciamento dos equipamentos e de todas as suas			• Pag. 8 – Switch_Tipo2_doc3 • Vide configuração, pág. 206 e 216 - módulo GigaStack GBIC (acompanha o cabo) • Pag. 2 – Switch_Tipo2_doc4 Pag. 14 – Switch_Tipo2_doc1 • Pag. 7 – Switch_Tipo2_doc1 • Pag. 12 – Switch_Tipo2_doc1 • Pag. 1 – Switch_Tipo2_doc5

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0413
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	interfaces através de aplicação gráfica; • Serão fornecidos servidores adicionais para a instalação desta gerência.			Switch_Tipo2_doc5 • Proposta Econômica pág. 211 para Brasília e 221 para São Paulo.
4 – Fonte de Alimentação	• Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação serão redundantes por fontes internas ou externas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.		Sim	• Pag. 16 – Switch_Tipo2_doc1 • Pag. 15 – Switch_Tipo2_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0241
Doc.

3.3. SWITCH TIPO 3 (FC)

Itautec

SW TIPO 3

MARCA: IBM

MODELO: SAN SWITCH 2109

FABRICANTE: IBM

OBJETIVO
Conectividade com os Storage Existente e Backup Robotizado

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento(Sim / Não)**	**Página da documentação Técnica**
1 – Recursos Básicos	▪ Serão diponibilizados equipamentos com 64 Portas Fibre Channel, operando a 2Gbit/sec, que serão interligados à rede SAN já existente na contratante. ▪ Os equipamentos fornecidos interligarão a todos elementos relativos a Storage Area Network - SAN, definidos: Servidores (Intel e RISC) fornecidos; Storage (IBM 2105 F20); Backup fornecido.STORAGE (IBM 2105 F20); BACKUP fornecido. • Os Swtiches possuem os seguintes recursos: Possibilidade de configuração das portas de forma		Sim	Manual 1 - SPEC SHEET pag. 01 e 02 Manual 07 pag. 1 Manual 1 - SPEC SHEET pag. 1 e 2 Manual 2 - Sup. Servers. Manual 1 - SPEC SHEET pag. 01,02 e 03

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	configuração das portas de forma independente; Portas são "HOT-SWAPPABLE/HOT-PLUGGABLE"; Modularidade. • Os Switches são montados em RACKS de 19";			Manual 1 - SPEC SHEET pag. 03
2 – Portas Ethernet	• Possui 1 (uma) interface Fast-Ethernet 10/100 autosensing, com protocolo SNMP para gerência.		Sim	Manual 1 - SPEC SHEET pag. 03 Manual 3 pag.3
3 – Cabeamento	• Serão disponibilizados e instalados, todos os recursos necessários ao cabeamento, incluindo os cabos, que são em Fibra Ótica Multi Mode com conectores LC.		Sim	Manual 1 - SPEC SHEET pag. 04 + Proposta Econômica
4 – Recursos	• Os equipamentos possuem todos os recursos de hardware, software, cabos, manuais, etc necessários a sua total instalação, configuração, gerenciamento e utilização. ▪ Possui ferramenta que implemente o gerenciamento da rede SAN, contemplando todos os agentes e consoles necessários ao	N/A	Sim	Declaração + Proposta Econômica Manual 1 - SPEC SHEET pag. 01 Tivoli

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 946
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	seu pleno funcionamento. ▪ Permite descoberta automática dos elementos que compõe a SAN, baseado em protocolo SNMP ou agente da própria ferramenta; ógica da topologia dos elementos que de forma gráfica, incluindo as , switches,servidores e devices de ica console; ▪ Possui a capacidade de apresentar detalhes sobre as conexões das portas FC; ▪ Possui a capacidade de receber eventos provenientes dos elementos constantes na topologia SAN; ▪ Possibilita o envio dos eventos recebidos através de protocolo SNMP ou agentes próprios. ▪ Serão montados 2(dois) ambientes de gerenciamento da Rede SAN, sendo 1(um) no CCD			Manual 1 - SPEC SHEET pag. 01 Manual 09 pag 04 Manual 10 pag. 02 Manual 1 - SPEC SHEET pag. 01 Manual 09 pag.05e 05 Manual 10 pag. 04 Manual 1 - SPEC SHEET pag. 01 Manual 09 pag. 29 Manual 1 - SPEC SHEET pag. 01 Manual 09 pag. v Manual 10 pag. Vii Manual 1 - Spec Sheet pag.3 Manual 10 pag. 113 e 114 Declaração

ECT CN CPMI - CORREIOS Fls. Nº 0417 Doc. ROS nº 03/2005

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	Brasília e 1 (um) no CCD de São Paulo. ▪ Fornece os servidores necessários para implementação da gerência da rede SAN.			Declaração Proposta Econômica Pag.160-161 e 167-168 Os serviços de implantação da gerência da rede SAN, referente à implantação do software SAN Manager está contemplado conforme descrito na "Etapa E04 - Instalação e Configuração do SAN Manager" do item "2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0485
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
				configuração de SAN Manager", conforme página 38.
5– Compatibilidade e Integração	• Os equipamentos são totalmente compatíveis e fornece suporte total aos padrões Fiber Channel. • Os equipamentos fornecidos integra aos equipamentos já existenes na contratante, formando uma única rede SAN em cada localidade Brasília-DF e São Paulo-SP. ıipamentos existentes são: ▪ Switches: Modelo IBM 2109-S16; Fabricante IBM (OEM Brocade 2800 Silkworm), versão de microcódigo A2.4.1C; ▪ Storage: Modelo 2105-F20 (IBM) com dois microcódigos (2 dispositivos de armazenamento): 1.5.2.103 e 1.3.2.49; ▪ HBA`s: modelo QLOGIC QLA 2200 - PCI Fibre Channel Adapter, versão de Microcódigo 8.0.8.1.		Sim	Manual 3 - pag.103 à 107 Manual 1- Spec Sheet pag.3 Manual 1- Spec Sheet pag.2 Manual 1- Spec Sheet pag.2 + Declaração Manual 1- Spec Sheet pag.2 + Declaração Manual 2 + Declaração (é que as placas no RISC FC 6227 é QLA 2200F Manual 4 pag.39 e 26

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 0349 Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
				Manual 2 + Declaração do Fabricante ; Manual 4 pag.39 e 26
6 – Fonte de Alimentação	• Fontes instaladas na configuração máxima do equipamento, com recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PUGGABLE) e alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, freqüência de 60 (sessenta) Hertz; • As fontes de alimentação são reduntantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.		Sim	Manual 1- Spec Sheet pag.2 e 4 Manual 3 pág. 30 e 103 Manual 1- Spec Sheet pag.2 e 4 Manual 03 pág. 30

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

3.4. SWITCH TIPO 4 (KVM)

MARCA: BLACKBOX

MODELO: SERVSWITCH AFFINITY

FABRICANTE: BLACKBOX

OBJETIVO
Comutação vídeo, mouse e teclado de todos os servidores do ambiente.

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento(Sim / Não)**	**Página da documentação Técnica**
1 – Descrição	• Serão fornecidas 2 (duas) redes de comutação de teclado, vídeo e mouse, sendo 1 (uma) rede no CCD de Brasília-DF e 1 (uma) rede no CCD de São Paulo-SP, devendo atender a todos os servidores da plataforma INTEL fornecidos, incluindo servidores legados existentes na ECT ; • Os equipamentos fornecidos serão compatíveis com a atual solução de comutação existente na ECT , fornecida pela empresa BLACKBOX (modelo: Affinity);		Sim	• Página 28 da proposta econômica do item – "Implementação de Servswitch" • Manual 27: Página de 1 a 2

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0951
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Os SWITCHES TIPO 4 serão montados em RACKS de 19" de acordo com o subitem 7, a serem fornecidos pela ITAUTEC; • O número e os locais de instalação dos RACKS serão indicados pela ECT ; • Permitirá, para os servidores da Plataforma INTEL, fornecidos pela ITAUTEC, a utilização de Hardware para Gerenciamento Remoto, em substituição aos equipamentos especificados acima, desde que as características deste hardware, descritas no Subitem 3.4.4. deste Anexo sejam atendidas.			• Manual 27: Página 2 • Página 28 da proposta econômica do item – "Implementação de Servswitch" • Manual 27: Página 1
– Quantidade de Portas	• O conjunto de equipamentos fornecidos para o CCD de Brasília disponibilizará um mínimo de 160 (cento e sessenta) portas de comutação, independente da quantidade de equipamentos que		Sim	Página 28 da proposta econômica do item – "Implementação de Servswitch"

ECT CPMI - CORREIOS Nº 0352 Doc. RQS nº 03/2005 - CN

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	utilizarão para atingir este número, respeitando o número mínimo de 16 (dezesseis) portas por equipamento; • O número mínimo de servidores legados que serão atendidos pela rede de comutação no CCD de Brasília é o seguinte: ▪ 24 Servidores RISC da Marca SUN Microsystems; ▪ 48 Servidores da Plataforma INTEL. • O conjunto de equipamentos fornecidos para o CCD de São Paulo disponibilizarão um mínimo de 96 (noventa e seis) portas de comutação, independente da quantidade de equipamentos que utilizarão para atingir este número, respeitando o número mínimo de 16 (dezesseis) portas por equipamento; • O número mínimo de servidores legados que serão atendidos pela rede de comutação no CCD de São Paulo é o seguinte:			Página 28 da proposta econômica do item – "Implementação de Servswitch" • Página 28 da proposta econômica do item – "Implementação de Servswitch" Página 28 da proposta econômica do item – "Implementação de Servswitch"

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0353
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ 48 Servidores da Plataforma INTEL.			
3 – Consoles	• Será disponibilizado um conjunto de 8 consoles externos à sala de segurança física para Brasília e um conjunto de 4 consoles externos à sala de segurança física para São Paulo; • As consoles serão independentes entre si, podendo acessar qualquer servidor, inclusive os servidores legados descritos no Subitem 3.4.2.; • As 12 (doze) consoles utilizarão monitores de vídeo que alcancem resolução de 1280x1024 60Hz com no mínimo com 17" (dezessete polegadas), policromático e DOT PITCH 0,28, mouse e teclado padrão ABNT2;		Sim	Página 28 da proposta econômica do item – "Implementação de Servswitch" • Página 28 da proposta econômica do item – "Implementação de Servswitch" • Manual 26: Página Web dos Componentes: Monitor P/N 31P8136 pag.69-72 Mouse P/N 28L3673 – Pág. 75 Declaração Comprobatória pg.89 • Manual 27:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Doc. 3
Fls. Nº 0541

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• As consoles serão montadas fora das Salas de Segurança Física de Brasília e São Paulo, a uma distância de aproximadamente 50 (cinqüenta) metros. Todos os materiais e componentes necessários a esta montagem serão fornecidos pela ITAUTEC.			Página 2 • Manual 26: Página Web dos Componentes: Monitor P/N 31P8136 pag.69-72 Mouse P/N 28L3673 – Pág. 75 Declaração Comprobatória pg.89 • Manual 27: Página 2 Página 28 da proposta econômica do item – "Implementação de Servswitch"
4 – Solução Alternativa para	• A ITAUTEC substituirá portas de comutação de teclado, vídeo e mouse por controladoras que		Sim	A Solução apresentada não necessita de uma solução alternativa, pois

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
comutação dos Servidores INTEL	permitam o Gerenciamento Remoto, para os servidores da plataforma INTEL fornecidos, de forma que 1 (uma) controladora de gerenciamento remoto substitui 1 (uma) porta de comutação solicitada; • O Hardware para Gerenciamento Remoto possuirá as seguintes características técnicas: ▪ Placa PCI instalada em slot do mesmo padrão ou integrada a placa – mãe; ▪ Funcionará independentemente do Sistema Operacional; ▪ Permitirá o acompanhamento e controle de todo o ciclo de inicialização do servidor, incluindo as etapas de POST (Power On Self Test) e carga do Sistema Operacional; ▪ Será do mesmo fabricante do servidor; ▪ Possibilitará a utilização de console remota gráfica através de browser; ▪ Implementará mecanismo de			atende a todos os requisitos deste Edital.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 9013
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	segurança para a comunicação entre o browser e o dispositivo de gerenciamento, através utilização do padrão SSL (Security Socket Layer) 128 bits; ▪ Possuirá interface Ethernet 10/100 Mbits ou superior dedicada, suportando alocação fixa de endereço IP; ▪ Possibilidade de ligar/desligar o servidor remotamente, para usuários autenticados; ▪ Implementará mecanismo de autenticação para usuários no próprio dispositivo de gerenciamento.			
5 – Gerais	• Para a conexão dos servidores à rede de comutação, a ITAUTEC fornecerá todos os cabos e acessórios necessários a esta operação • Os cabos de interligação dos equipamentos fornecidos ao computador terão comprimento possuirão o comprimento suficiente para interligar todos os		Sim	Página 28 da proposta econômica do item – "Implementação de Servswitch" Página 28 da proposta econômica do item – "Implementação de Servswitch"

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 0127
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	suficiente para interligar todos os equipamentos, entretanto, os cabos utilizados para conectar servidores legados devem ter comprimento mínimo de 15 (quinze) metros;			
	• Os cabos a serem oferecidos terão comprimento suficiente para permitir a conexão a qualquer servidor, considerando as características dos equipamentos ofertados;			Página 28 da proposta econômica do item – "Implementação de Servswitch"
	• Os equipamentos utilizados na rede de comutação devem estar cascateados, de modo que, a partir de qualquer uma das consoles seja possível o acesso a qualquer equipamento conectado nas redes de comutação fornecidas;			Página 28 da proposta econômica do item – "Implementação de Servswitch"
	• A escolha do servidor a ser comutado deve ser feita por menu configurável, utilizando os nomes dos servidores designados pela ECT ;			Página 28 da proposta econômica do item – "Implementação de Servswitch"
	• Os equipamentos possuirão			• Manual 27:

ROS nº 03/2005 CN CPMI CORREIOS
Fls. Nº 0155
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	alimentação elétrica de acordo com a localidade onde instalarão, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz.			Página 2

3.5 SWITCH TIPO 5 (CONCENTRADOR DE VPNs)

MARCA: CISCO

MODELO: VPN 3060-HA-K9

FABRICANTE: CISCO

OBJETIVO
Viabilizar acessos externos de forma segura.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – Descrição	• O Switch operará como concentrador VPN, devendo ser composto por sistema integrado de hardware e software, com objetivo de concentrar, configurar e monitorar acessos remotos via		Sim	• Pag. 1 – Switch_Tipo5_doc1

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0119
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	VPN.			
2 – Características e Funcionalidades do Sistema	• Capacidades de firewall; • Suporte aos protocolos de tunelamento PPTP, IPsec, L2TP, L2TP/IPsec for Windows 2000, NAT transparent IPSEC; • O suporte a serviços deve ser estendido a todo e qualquer serviço que funcione sobre o protocolo IP, com a possibilidade de customização; • Suporte a certificados digitais padrão X.509 v.3; • Alta disponibilidade, com redundância e capacidade de tolerância à falhas (failover); • Suporte ao gerenciamento de chaves do tipo IKE; • Capacidade de registrar eventos e de envio de notificações por e-		Sim	• Pag. 4 – Switch Tipo5 doc1 • Pag. 5 – Switch_Tipo5_doc1 • Pag. 1 – Switch_Tipo5_doc6 • Pag. 5 – Switch_Tipo5_doc1 • Pag. 7 – Switch_Tipo5_doc1 • Pag. 4 – Switch_Tipo5_doc1 • Pag. 6 – Switch_Tipo5_doc1 • Pag. 6 – Switch_Tipo5_doc1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 9960
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	mail; • Suporte aos protocolos de roteamento RIP, RIP2, OSPF estático; • Permitirá que as configurações e políticas de acesso sejam aplicadas ao cliente no momento em que a conexão for estabelecida; • A configuração física do concentrador VPN possuirá no mínimo 3 interfaces 10BaseT/BaseTX; • O equipamento deve integrar-se com um sistema de autenticação externa, o qual será dimensionado, fornecido e configurado pela IBM (hardware e software) com as seguintes características: • Capacidade de Autenticação de no mínimo 5.000 usuários;			• Pag. 6 – Switch_Tipo5_doc1 • Pag. 3 – Switch_Tipo5_doc1 • Pag. 5 – Switch_Tipo5_doc1 • Pag. 7 – Switch Tipo5 doc1 e Pag. 1 – Switch Tipo5 doc2 • Pag. 3 – Switch_Tipo5_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0035
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Suporte ao padrão LDAP; • Integração com o domínio Microsoft Windows da Contratante, compartilhando bases de grupos, usuários e permissões • Permitirá configuração de níveis de acesso administrativos; • Permitirá a configuração e aplicação de políticas de segurança nas estações clientes; • Capacidade de gerenciamento de política para usuários e grupos; • Controle de tempo e horário de acesso do usuário; • Suporte ao gerenciamento utilizando SNMP MIB-II; • Oferece ferramenta de gerenciamento que possibilite verificação de estatísticas de			• Pag. 7 – Switch Tipo5 doc1 e Pag. 3 – Switch Tipo5 doc2 • Pag. 7 – Switch Tipo5 doc1 e Pag. 4 – Switch Tipo5 doc2 • Pag. 6 – Switch_Tipo5_doc1 • Pag. 3 – Switch_Tipo5_doc1 • Pag. 4 – Switch_Tipo5_doc1 • Pag. 7 – Switch_Tipo5_doc1 • pág. 6 – Switch_Tipo5_doc1 • pág. 6 – Switch_Tipo5_doc1

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	tráfego criptografado, negociações de handshake e resposta a pacotes; • Possibilidade de crescimento (escalabilidade) conforme demanda, com configuração e gerência centralizada; • Capacidade de geração de relatórios gerenciais, com informações como: número de túneis estabelecidos, tráfego transferido, clientes com maior geração de tráfego, entre outras.			• pág. 1 e 2 – Switch_Tipo5_doc11 • pág. 4 – Switch_Tipo5_doc11 • pág. 3 – Switch_Tipo5_doc19 • Pag. 18 – Switch_Tipo5_doc7 Pag. 2 – Switch_Tipo5_doc8
2 – Características e Funcionalidades do Sistema (continuação)	• O sistema de gerenciamento do SWITCH TIPO 5, será disponibilizado pela IBM em hardware do tipo servidor, de forma exclusiva, sendo 01 (um) sistema para o CCD de Brasília-		Sim	• Pag. 1 – Switch Tipo5 doc9 ; Pag. 3 – Switch Tipo5 doc9 ; Pag. 13 – Switch Tipo5 doc9

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0833
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	DF e 01 (um) sistema para o CCD de São Paulo-SP. Tal sistema, poderá estar integrado em um mesmo framework dos SERVIDORES DE SEGURANÇA LÓGICA TIPO 1 e TIPO 2, ROTEADOR TIPO 1 e SISTEMA DE DETECÇÃO DE INTRUSÃO.			
3 – Características e Funcionalidades do Software Cliente VPN	• Número mínimo de 5.000 licenças; • Auto-atualização, realizando atualizações automáticas sem necessidade da intervenção do usuário; • Personal firewall; • Suporte aos sistemas operacionais Windows 95, 98, ME, NT 4.0, 2000 e XP;		Sim	• pág. 1– Switch Tipo5 doc4 ; Pag. 3 – Switch Tipo5 doc1 • pág. 1 e 2– Switch_Tipo5_doc4 • pág. 2– Switch_Tipo5_doc4 • pág. 2– Switch Tipo5 doc4 ; Pag. 3– Switch Tipo5 doc10

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Interface padronizada, com o logotipo da Itautec.			• pág. 1 – Switch_Tipo5_doc3
4 – Características de Desempenho	• Capacidade de tratar no mínimo 5.000 usuários simultâneos; • Possuirá capacidade de processamento de encriptação mínima de 100Mbps.		Sim	• pág. 3 – Switch_Tipo5_doc1 • pág. 3 – Switch_Tipo5_doc1
5 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação serão redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em		Sim	• pág. 8 – Switch_Tipo5_doc1 • pág. 8 – Switch_Tipo5_doc5 • Declaração do Fabricante - CISCO • pág. 8 – Switch_Tipo5_doc1 • pág. 8 –

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0965
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.			Switch_Tipo5_doc5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3608
Doc.

3.6. ROTEADOR TIPO 1

MARCA: CISCO

MODELO: 3745 MULTISERVICE ACCESS ROUTER

FABRICANTE: CISCO

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – Router	• Possuirá estrutura de chassis modular com pelo menos 04 (quatro) slots para inserção de módulos e interfaces; • O ROTEADOR TIPO 1 serão montados em RACK de 19" de acordo com o Subitem 7, a ser fornecido pela Itautec.		Sim	• pág 2 - Roteador_Tipo1_Doc1 • pág 3 - Roteador_Tipo1_Doc1
2 – Processamento	• Possuirá capacidade de roteamento de pelo menos 225.000 (duzentos e vinte e cinco mil) pps, utilizando pacotes de 64 (sessenta e quatro) bytes, sem perda de pacotes.		Sim	• pág 11 - Roteador_Tipo1_Doc1
3 – Interfaces	• Possuirá no mínimo 03 (três) interfaces 10/100Base-TX, fast ethernet, full duplex, para cabos		Sim	• pág 11 - Roteador_Tipo1_Doc1

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 0361 Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	UTP Categoria 5 e conectores RJ-45; • Possuirá no mínimo 8 (oito) interfaces seriais síncronas V.35 de alta velocidade (até 2Mbps); • Possuirá no mínimo 02 (duas) interfaces ATM E3, compatível com o padrão ITU-T G-703; • Possuirá no mínimo 1 (uma) interface Gigabit 1000Base-T.			Proposta Econômica Pág 209 e 220 Proposta Econômica Pág 209 e 220 Proposta Econômica Pág 209 e 220
4 – Geral	• Possuirá MTBF (Mean Time Between Failures) de pelo menos 50.000 (cinqüenta mil) horas; • Permitirá o seu gerenciamento através de aplicação gráfica; • Implementará o protocolo SNMP, incluindo a geração de traps; • Gerenciável através de protocolo SNMP e possuirá suporte a MIB II, conforme RFC 1213;		Sim	Declaração do Fabricante - CISCO • pág 4 - Roteador_Tipo1_Doc11 Pag 1 - Roteador_Tipo1_Doc12 • pág 18 - Roteador_Tipo1_Doc2 • pág 3 - Roteador_Tipo1_Doc3

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Possui descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;			• Roteador_Tipo1_Doc3
	• Implementará Telnet para acesso à interface de linha de comando;			• pág 7 - Roteador_Tipo1_Doc7
	• Implementará o protocolo SSH;			• pág 17 - Roteador_Tipo1_Doc2
	• Possuirá proteção contra ataques de Denial of Service do tipo TCP SYN Attack;			• pág 3 - Roteador_Tipo1_Doc1
				• pág 9 - Roteador_Tipo1_Doc2
	• Implementará IPSec padrão IETF com criptografia Triple DES;			• pág 1 - Roteador_Tipo1_Doc12
	• Suporte para SYSLOG EXTERNO, que será dimensionado e fornecido pela IBM, em hardware à parte;			• Proposta Econômica Pág 209 e 220
	• O hardware a ser especificado e fornecido pela IBM no item anterior, caso seja do tipo Servidor, disponibilizará, no			• pág 3 -

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 0069 Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	mínimo, 1 (uma) Controladora FIBER CHANNEL, operando a 2Gb/s, de forma se possa conectar este servidor a rede SAN fornecida; • Permitirá a atualização dos softwares utilizados no equipamento através de rede; • Implementará mecanismo de autenticação para acesso ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS ou TACACS; • Protege a interface de comando do equipamento através de senha; • Implementará o protocolo VRRP, ou similar, em todas as interfaces disponibilizadas; • Implementará o protocolo PIM para roteamento de multicasts; • Implementará roteamento IP usando os protocolos OSPF, RIP, RIP2 e BGP-4;			Roteador_Tipo1_Doc5 • pág 16 e 20 - Roteador_Tipo1_Doc2 • pág 13 - Roteador_Tipo1_Doc6 • pág 8 - Roteador_Tipo1_Doc2 • pág 15 - Roteador_Tipo1_Doc2 • pág 2, 14, 20, - Roteador_Tipo1_Doc2 • pág 5 - Roteador_Tipo1_Doc2 • Declaração do Fabricante - CISCO

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Implementa DHCP; • Permitirá a configuração de pelo menos 1024 (mil e vinte e quatro) rotas estáticas; • Implementará Policy-Based Routing; • Implementará filtros para redistribuição de rotas entre RIP, OSPF e BGP-4; • Implementará as seguintes características para o protocolo BGP-4: Route Reflectors, Route Confederations, Route Aggregation, IGP Synchronization e Route Flap Dampening.			• pág 15 - Roteador_Tipo1_Doc2 • pág 3 -Roteador Tipo1 Doc2 ; pág 1 -Roteador Tipo1 Doc10 • pág 24,24, 19, 10, 34 - Roteador_Tipo1_Doc8
4 – Geral (continuação)	• Permitirá a configuração de Policy-Based Routing baseado no endereço de origem da rede; • Suportará a implementação de NAT (Network Address Translation); • Suportará inserção em redes com		Sim	• pág 2 - Roteador_Tipo1_Doc9 • pág 13 - Roteador_Tipo1_Doc2

Fls. Nº
Doc.
RCS nº 03/2005 - CN
CPMI - CORREIOS

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	serviços de Voz sobre IP (VoIP) e Voz sobre Frame-Relay (VoFR); • Suportará os protocolos G.711 e G.729 para tráfego de voz. e funcionar como gateway H.323 para suporte de configuração de chamada de videoconferência; • A Itautec fornecerá ferramentas que permitam o gerenciamento dos equipamentos e de todas as suas interfaces através de aplicação gráfica; • Serão fornecidos servidores adicionais para a instalação desta gerência.			• pág 5 - Roteador_Tipo1_Doc1 • pág 7 -Roteador Tipo1 Doc4 ; pág 13 – Roteador Tipo1 Doc2 • pág 1 - Roteador_Tipo1_Doc12 Proposta Econômica Pág 211 e 221
5 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5. deste ANEXO, freqüência de 60		Sim	Proposta Econômica Pág 209 e 220 • pág 4 - Roteador_Tipo1_Doc1 • pág 12 - Roteador_Tipo1_Doc1

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº
Doc

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	(sessenta) Hertz; • As fontes de alimentação devem ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.			Proposta Econômica Pág 209 e 220

3.7. ROTEADOR TIPO 2

MARCA: CISCO

MODELO: 1751-V ROUTER

FABRICANTE: CISCO

OBJETIVO
Prover a conectividade dos equipamentos do ambiente de testes e homologação.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
1 – Router Processamento	• Possuirá capacidade de no mínimo 12 Kpps. • O ROTEADOR TIPO 2 deve ser montados em bandejas instaladas no interior do RACK de 19" de acordo com o Subitem 7 deste ANEXO, a ser fornecido pela ITAUTEC		Sim	Declaração do Fabricante - CISCO • Pág. 18 – Roteador_Tipo2_doc1
2 – Gerenciamento	• Será gerenciável via SNMP(v1, v2 e v3), Telnet e acesso local. Possuirá suporte a MIB II, conforme RFC 1213.		Sim	• pág. 6 – Roteador Tipo2 doc1 ; Pag 2 - Roteador Tipo2 doc3
3 – Interfaces	• Possuirá no mínimo 1 (uma) interface Ethernet, 10BASE-T/100BASE-TX, com detecção automática, integrada ao chassis para conexão com a LAN através de interface RJ-45. • Possuirá no mínimo 2 (duas) interfaces seriais para conexão/simulação de um ambiente WAN, sendo uma do tipo DCE e outra do tipo DTE, com conectores V.35 ou		Sim	• pág. 10 – Roteador_Tipo2_doc1 pág. 10 – Roteador_Tipo2_doc1 Proposta Econômica Pág 209 e 220

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0214
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	EIA/TIA-232, com compressão e encriptação de dados, sem necessidade de interfaces ou dispositivos externos. • Devem ser fornecidos os cabos e demais acessórios necessários à conexão das interfaces seriais, de maneira a Implementar as interfaces do tipo DCE e DTE nestes roteadores.			Proposta Econômica Pág 209 e 220
4 – Gerais	• Possui sinalização visual de funcionamento e "status" das portas. • Permitirá a atualização dos softwares utilizados no equipamento através da rede. • Deve suportar e implementar recursos de QoS avançados, como Committed Access Rate (CAR), Custom, Low Latency Fair Queueing and Weighted Fair Queuing (WFQ), Bandwidth on Demand (BoD), Resource Reservation Protocol (RSVP),		Sim	• pág. 7 – Roteador_Tipo2_doc1 • pág. 18 – Roteador_Tipo2_doc4 • pág. 7 – Roteador_Tipo2_doc1 Roteador_Tipo2_doc2

ROS nº 03/2005 - CN
CPMI - CORREIOS
Doc.
Fls. Nº

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	Weighted Random Early Detection (WRED), Policy Based Routing, Frame Relay Fragmentation (FRF.12), e RTP compression (cRTP).			
	• Implementará e permitirá o roteamento entre VLANs, suportando o padrão 802.1Q.			• pág. 6 – Roteador_Tipo2_doc1
	• Permitirá VPN Tunneling com IPSec, L2TP e L2F.			• Pag. 6 – Roteador_Tipo2_doc1
	• Permitirá roteamento IP usando os protocolos OSPF, RIP, RIPv2 e BGP-4, PIM Dense e Sparse Mode.			• Roteador_Tipo2_doc2
	• Suportará à criptografia 3DES.			• pág. 6 – Roteador_Tipo2_doc1
	• Suportará autenticação através dos protocolos RADIUS, TACACS+ e PAP/CHAP.			• pág. 8 – Roteador_Tipo2_doc1
	• Suportará inserção em redes com serviços de Voz sobre IP (VoIP) e Voz sobre Frame-Relay (VoFR).			• pág. 17 – Roteador_Tipo2_doc1
	• Terá as funcionalidades de firewall, incluindo ACLs e			• pág. 8 – Roteador_Tipo2_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0346
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	AAA,criptografia, VPN tunnel server, integradas ao roteador. • Suportará comunicação de voz digital e analógica na infra-estrutura telefônica existente (telefones, fax e PBXs), sem gasto com equipamentos adicionais. • Possuirá duas interfaces do tipo Foreign Exchange Station (FXS) para conexão de telefones analógicos e duas interfaces do tipo Foreign Excange Office (FXO) para conexão em interfaces de ramal de um PABX. • Possuirá alimentação elétrica de 90 a 240 Volts com comutação automática, freqüência de 60 (sessenta) Hertz.			• pág. 3 – Roteador_Tipo2_doc1 pág. 3 – Roteador Tipo2 doc1 Proposta Econômica Pág 209 e 220 Declaração do Fabricante - CISCO

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0171
Doc.

Itautec

4. SERVIDORES CORPORATIVOS

4.1. SERVIDORES INTEL

4.1.1. SERVIDORES INTEL TIPO 1

MARCA: IBM

MODELO: x440

FABRICANTE: IBM

OBJETIVO
Banco de Dados de Grande Porte e Correio Eletrônico Corporativo

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento (Sim/Não)**	**Página da documentação Técnica**
1 – CPU e Performance	• Servidor composto por processadores Intel, com 8 (oito) processadores INTEL XEON MP, com clock de 2,0 GHz, sem a formação de Cluster; • O equipamento possui performance 119.115 tpm-C, conforme especificado	• Adicional de 29.115 tpm-C. • Rack com altura máxima de 42U.	SIM	Manual 26: xRef - Pag. 03 Componentes : - P/N : 59P5173 – Pag. 07 - P/N : 59P5188 – Pag. 09 Página Web

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 0185
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	no Subitem 2.2.; • O equipamento será montado em RACK próprio do fabricante com 42U de altura.			www.tpc.org Pag. 04 Página Web do Rack – Pag. 65-68 Proposta Econômica
2 – Barramento	• Barramento do sistema de 400 MHz.		SIM	Manual 26: xRef - Pag 03 Componente : - P/N : 59P5173 – Pag. 07
3 – Memória Cache	• 2MB (dois Megabytes) por processador	O servidor ofertado possui também o Cache L4, que é externo aos caches do processador, com capacidade de 64MB.	SIM	Manual 26: xRef - Pag 03 Componente : - P/N : 59P5173 – Pag. 07
4 – Memória RAM	• 8 GB (oito gigabytes) ECC SDRAM.	Além de suportarem as características de ECC SDRAM, são memórias RDIMM, 4-way interleave, cujo sistema suporta as tecnologias Chipkill Memory,	SIM	Manual 26: xRef – Pag, 03 Componente : - P/N : 33L3324 – Pag. 11

ROS nº 03/2005 - CN
CPMI - CORREIOS
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
		Memory ProteXtion e, opcionalmente, Active Memory (Espelhamento de memória) que pode ser ativado no "Set up" do equipamento.		
5 – Controladora e Unidade de Disco Rígido – Interno	▪ Capacidade em disco de 72 GB (líquidos) após implementado um arranjo em RAID 1 por hardware utilizando discos com tempo médio de acesso igual a 4,9 ms e velocidade de rotação de 10.000 RPM. ▪ Controladora de discos padrão Ultra 3 / Ultra 160 SCSI, com suporte a troca de discos defeituosos sem interrupção no funcionamento do equipamento. ▪ Controladoras de disco instalada em slot PCI-	• Os discos ofertados suportam o padrão Ultra160 SCSI com 10.000 RPM e um tempo médio de acesso de 4,9ms. • Controladora SCSI RAID Ultra 160 com 32MB de cache, PCI 64bit, 66MHz.	SIM	Manual 26: Página Web dos componentes : - HDD P/N : 06P5756 - Pag. : 47/48 - Control. SCSI RAID : P/N : 06P5740 – Pag. 49-55 Proposta Econômica Pág 210 e 220

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0181
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	X.			
6 – Interface de VIDEO	• Padrão SVGA, PCI 32 Bits, com 8 Mbytes.		SIM	Manual 26: xRef – Pag. 3 Declaração – Pag. 63
7 – Unidade de CD/DVD-ROM	• 1 (uma) unidade interna, tecnologia IDE, com velocidade de 24X CD-ROM.		SIM	Manual 26: xRef – Pag. 03
8 – Controladora de I/O (por equipamento)	• Serão disponibilizadas controladoras FIBER CHANNEL, operando a 2Gb/s, para acesso à Rede SAN, com disponibilidade para 2 (dois) canais; • Serão disponibilizadas 3 (três) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP.; • As interfaces de rede conectarão os servidores a Rede do CCD utilizando cabeament UTP CAT-6 e		SIM	Manual 26: Página Web dos componentes : - Fiber Channel HBA P/N : 24P0960 - Pag. : 57 - Placa Ethernet 10/100/1000 BaseT: P/N : 36P6301 – Pag. 59 - NetXtreme Gigabit Ethernet Adapter User's Guide : Pag. 61 Proposta Econômica item 1.3.1 pág 8

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0381
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	conectores RJ-45.			
9 – Ambiente Operacional	• Os Servidores INTEL TIPO 1 serão fornecidos com o seguinte ambiente operacional para cada equipamento: ▪ Microsoft Windows Server 2003 Enterprise Edition, com número ilimitado de usuários simultâneos, instalado, licenciado e configurado para Rede Corporativa dos Correios;	•	Sim	O Sistema Operacional Microsoft Windows Server 2003 Enterprise Edition a ser licenciado é conforme endereço internet http://www.microsoft.com/catalog/display.asp?subid=22&site=11261, e será instalado e configurado conforme "Etapa E02 - Instalação e Configuração do ambiente Plataforma Windows 2000/2003" do item "2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
				Cluster Service e Instalação e configuração de SAN Manager", conforme página 38.
	▪ 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios;			O Agente SysEdge a ser licenciado é conforme endereço internet http://www.concord.com, e será instalado e configurado conforme item "2.7 - Implementação do gerenciamento eHealth Enhanced Sysedge, conforme página 63.
	▪ 1 (uma) licença de software agente de backup compatível com o software gerenciador de fitoteca especificado no Subitem 5.13 que permita backup LAN			Manual 26: IBM Tivoli Storage Manager for Windows Storage Agent User's Guide, página 1 – pag. 79-82.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0233
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	FREE, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; • Será fornecido, na modalidade de licenciamento por CPU, para uso perpétuo, o SGBD MICROSOFT SQL SERVER 2000 ENTERPRISE EDITION para 7 (sete) servidores INTEL TIPO 1. O SGBD será instalado e configurado em Cluster pela Itautec, utilizando o recurso de cluster do sistema operacional, de acordo com a configuração definida pela ECT .			Manual 44 – IBM Tivoli Storage Manager for DataBases 5.1.5 Data Protection for MS SQL Server Installation and User´s Guide pág.1 Manual 26: IBM Tivoli Storage Manager for Windows Storage Agent User's Guide, página 1 – pag. 91-94. O SGBD Microsoft SQL Server 2000 Enterprise Edition a ser licenciado é conforme endereço internet http://www.microsoft.com/catalog/display.asp?subid=22&site=10145&x=41&y=19, e será instalado e configurado conforme "Etapa E03 - Instalação e

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 964
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
				Configuração de MS Cluster Service", do item "2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager", conforme pág. 38.
10 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Suporte ao recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possui alimentação elétrica de 220V em cada localidade onde serão instalados os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz;	Fontes de alimentação com suporte a auto-restart.	Sim	Manual 26: xRef – Pag. 03 Página Web do componente : - Manual HMM : Pag. 13-15

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0965
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento (Sim/Não)	Página da documentação Técnica
	• As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.			

4.1.2. SERVIDORES INTEL TIPO 2

MARCA: IBM

MODELO: x360

FABRICANTE: IBM

Doc. 3008
Fls. Nº 0866
RQS nº 03/2005 - CN CPMI - CORREIOS

OBJETIVO
Banco de Dados de Médio Porte e Aplicações Corporativas

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – CPU e Performance	• Servidor composto por processadores Intel, com no mínimo 4 (quatro) processadores INTEL XEON MP, com clock mínimo de 2,0 GHz, sem a formação de Cluster; • O equipamento deve apresentar performance mínima de 50.000 tpm-C, conforme especificado no Subitem 2.2.; • O equipamento deve ser montado em RACK próprio do fabricante com, no mínimo, 40U de altura.		Sim	Manual 26: xRef - Pag. 19 Componentes :P/N : 59P6817 – Pag. 23 Página Web www.tpc.org Pag. 21 Página Web do Rack – Pag. 65-68 Proposta Econômica pág. 200 e 201
2 – Barramento	• Barramento do sistema de, no mínimo, 400 MHz.		Sim	Manual 26: xRef - Pag 19 Componente : P/N : 59P6817 – Pag. 23
3 – Memória Cache	• 2MB (dois Megabytes) por processador.		Sim	Manual 26: xRef - Pag 19 Componente :

IRQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 0381
Doc.

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
				P/N : 59P6817 – Pag. 23
4 – Memória RAM	• 4 GB (quatro gigabytes) ECC SDRAM ou tecnologia superior,instalada.	Memórias padrão PC1600 (200MHz), DDR SDRAM RDIMM, 4-way interleave e tecnologia Chipkill Memory.	Sim	Manual 26: xRef – Pag, 19 Componente : P/N : 33L3283 – Pag. 25
5 – Controladora e Unidade de Disco Rígido – Interno	• Capacidade em disco de, no mínimo, 72 GB (líquidos) após implementado um arranjo em RAID 1 por hardware utilizando discos com tempo médio de acesso menor ou igual a 6 ms e velocidade de rotação mínima de 10.000 RPM. • Controladora de discos padrão Ultra 3 SCSI ou superior , com funcionalidade que permita a troca de discos ou periféricos defeituosos sem interrupção no funcionamento do equipamento. • São aceitas controladoras de disco instaladas na placa de sistema.	• Os discos ofertados suportam o padrão Ultra160 SCSI com 10.000 rpm e um tempo médio de acesso de 4,9ms. • Controladora SCSI RAID Ultra 160 com 32MB de cache, PCI 64bit, 66MHz.	Sim	Manual 26: Página Web dos componentes : HDD P/N : 06P5756 - Pag.: 47/48 Control. SCSI RAID: P/N : 06P5740 – Pag. 49-55

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0883
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
6 – Interface de VIDEO	• Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.		Sim	Manual 26: xRef – Pag. 19 Declaração – Pag. 63
7 – Unidade de CD/DVD-ROM	• 1 (uma) unidade interna, tecnologia IDE ou SCSI, com velocidade mínima de 24X CD-ROM ou 4X DVD-ROM.		Sim	Manual 26: xRef – Pag. 19
8 – Controladora de I/O (por equipamento)	• Devem ser disponibilizadas controladoras FIBER CHANNEL, operando a 2Gb/s, para acesso à Rede SAN, com disponibilidade mínima para 2 (dois) canais; • Devem ser disponibilizadas 2 (duas) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP;		Sim	Manual 26: Página Web dos componentes : Fiber Channel HBA P/N : 24P0960 - Pag. : 57 - Placa Ethernet 10/100/1000 BaseT: P/N : 36P6301 – Pag. 59- NetXtreme Gigabit Ethernet Adapter User's Guide : Pag. 61

RQS nº 03/2005 - CN - CORREIOS
Fls Nº 0989
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• As interfaces de rede devem conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.			Proposta Econômica – pág. 210 e 220 Proposta Econômica item 1.3.1 pág 8
9 – Ambiente Operacional	Os Servidores INTEL TIPO 2 devem ser fornecidos com o seguinte ambiente operacional para cada equipamento: ▪ Microsoft Windows Server 2003 Enterprise Edition, com número ilimitado de usuários simultâneos, instalado, licenciado e configurado para Rede Corporativa dos Correios;		Sim	O Sistema Operacional Microsoft Windows Server 2003 Enterprise Edition a ser licenciado é conforme endereço internet http://www.microsoft.com/catalog/display.asp?subid=22&site=11261, e será instalado e configurado conforme "Etapa E02 - Instalação e Configuração do ambiente Plataforma Windows 2000/2003" do item "2.4 Descrição dos Serviços de Instalação do Ambiente

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3600
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios;			Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager", conforme página 38. O Agente SysEdge a ser licenciado é conforme endereço internet http://www.concord.com, e será instalado e configurado conforme item "2.7 - Implementação do gerenciamento eHealth Enhanced Sysedge, conforme página 63.
	▪ 1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado			Manual 26: IBM Tivoli Storage

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 3008
Doc.

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios.			Manager for Windows Storage Agent User's Guide, página 79-86
10 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE); • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação devem ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.	Fontes de alimentação com suporte a auto-restart.	SIM	Manual 26: xRef – Pag. 19 Página Web do componente : - P/N : 31P6108 – Pag. 27 - Manual x360 User's Reference : Pag. 29-31 Proposta Econômica Pág 210 e 220.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3067
Doc.

4.1.3. SERVIDORES INTEL TIPO 3

MARCA: IBM

MODELO: x325

FABRICANTE: IBM

OBJETIVO
Banco de Dados de Pequeno Porte, Servidores de Aplicação e Serviços de Rede

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – CPU e Performance	• Servidor composto por processadores Intel, com no mínimo 2 (dois) processadores INTEL XEON, com clock mínimo de 2,4 GHz; • O equipamento deve apresentar performance mínima de 30.000 tpm-C, conforme especificado no Subitem 2.2.; • O equipamento deve ser montado em RACK próprio do fabricante com, no mínimo, 40U de altura.	Processadores Intel Xeon com clock de 3,06GHz	SIM	Manual 26: xRef - Pag. 35 Componentes : P/N : 02R1988 – Pag. 39 Proposta Econômica Página Web do servidor equivalente: www.tpc.org

ECT - CORREIOS - CPMI - RQS nº 03/2005
Fls. Nº 0903
Doc. 3602

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
				Pag. 37 Cálculo :Tpm-C estimado = tpm-C auditado= 18.936 * (no. De CPU ofertadas= 2 / no. CPU auditada = 1Tpm-C estimado = 37.872Página Web do Rack – Pag. 65-68
2 – Barramento	• Barramento do sistema de, no mínimo, 533 MHz.		SIM	Manual 26: xRef - Pag 35 Componente : P/N : 02R1988 – Pag. 39
3 – Memória Cache	• 512kB por processador.		SIM	Manual 26: xRef - Pag 35 Componente : P/N : 02R1988 – Pag. 39
4 – Memória RAM	• 1,5GB (um gigabyte e meio) ECC SDRAM ou tecnologia superior, instalada	Memórias padrão PC2100 (266MHz), DDR DIMM	SIM	Manual 26:

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 0994
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	instalada.	suportando 2-way interleave e Chipkill Memory.		xRef – Pag, 35 Componente : P/N : 33L5038 – Pag. 41 Proposta Econômica pág. 210 e 220.
5 – Controladora e Unidade de Disco Rígido– Interno	• Capacidade em disco de, no mínimo, 72 GB (líquidos) após implementado um arranjo em RAID 1 por hardware utilizando discos com tempo médio de acesso menor ou igual a 6 ms e velocidade de rotação mínima de 10.000 RPM. • Controladora de discos padrão Ultra 3 SCSI ou superior , com funcionalidade que permita a troca de discos ou periféricos defeituosos sem interrupção no funcionamento do equipamento. • São aceitas controladoras de disco instaladas na placa de sistema.	• Os discos ofertados suportam o padrão Ultra160 SCSI com 10.000 rpm e um tempo médio de acesso de 4,9ms. • Controladora Ultra 320 SCSI com capacidade de implementação de RAID 01 simples (espelhamento de apenas 02 discos).	SIM	Manual 26: Página Web dos componentes : HDD P/N : 06P5756 - Pag. : 47 Control. SCSI RAID on board : xRef – Pag. 35
6 – Interface de VIDEO	• Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.			Manual 26: xRef – Pag. 35

Doc. ____ Fls. Nº 0395 RQS nº 03/2005 - CN CPMI - CORREIOS

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
7 – Unidade de CD/DVD-ROM	• 1 (uma) unidade interna, tecnologia IDE ou SCSI, com velocidade mínima de 24X CD-ROM ou 4X DVD-ROM.	Unidade de CD-ROM 48x-20x IDE	SIM	Manual 26: xRef – Pag. 35
8 – Controladora de I/O (por equipamento)	• Devem ser disponibilizadas 2 (duas) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP.; • As interfaces de rede devem conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.		SIM	Manual 26: Página Web do componente : Placa Ethernet 10/100/1000 BaseT: P/N : 36P6301 – Pag. 59 NetXtreme Gigabit Ethernet Adapter User's Guide : Pag. 61 Proposta Econômica item 1.3.1 pág 8
9 – Ambiente Operacional	• Os Servidores INTEL TIPO 3 devem ser fornecidos com o seguinte		Sim	

ECT-MF Doc. 3668 ROS 0092005 - CN CPMI - CORREIOS 0968

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	ambiente operacional para cada equipamento: ▪ Microsoft Windows Server 2003 Standard Edition, com número ilimitado de usuários simultâneos, instalado, licenciado e configurado para Rede Corporativa dos Correios;			O Sistema Operacional Microsoft Windows Server 2003 Enterprise Edition a ser licenciado é conforme endereço internet http://www.microsoft.com/catalog/display.asp?subid=22&site=11261, e será instalado e configurado conforme "Etapa E02 - Instalação e Configuração do ambiente Plataforma Windows 2000/2003" do item "2.4 Descrição dos Serviços de Instalação do Ambiente na Plataforma Windows 2000/2003, Implementação de MS Cluster Service e Instalação e configuração de SAN Manager" conforme

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0971
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ 1 (uma) licença do agente 'Concord SystemEdge', devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; ▪ 1 (uma) licença de software agente de backup compatível com o gerenciador de fitoteca especificado no subitem 5.13, devidamente instalado e configurado conforme orientação da equipe técnica dos Correios.			Manager", conforme página 38. O Agente SysEdge a ser licenciado é conforme endereço internet http://www.concord.com, e será instalado e configurado conforme item "2.7 - Implementação do gerenciamento eHealth Enhanced Sysedge, conforme página 63. Manual 26: IBM Tivoli Storage Manager for Windows Storage Agent User's Guide, página 79-86.
10 – Fonte de Alimentação	• Instalada na configuração máxima do equipamento; • Recurso de troca sem interrupção	Fontes de alimentação com suporte a auto-restart.	SIM	Manual 26: xRef – Pag. 35

ECT/SRQS nº 83/2005 - CN - CPMI - CORREIOS
Fls. Nº 0098
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	(HOT-SWAPPABLE/HOT-PLUGGABLE); • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz; • As fontes de alimentação devem ser redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.			Página Web do componente : - x235 : User's Guide : Pag. 43-45

RQS nº 03/2005 - CN CPMI - CORREIOS
Doc. 3668
Fls. Nº 0990

Itautec

4.2. SERVIDORES RISC

4.2.1 SERVIDORES RISC TIPO 1

MARCA: IBM

MODELO: p690

FABRICANTE: IBM

-

OBJETIVO
Banco de Dados e aplicações corporativas.

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento(Sim / Não)**	**Página da documentação Técnica**
1 – CPU e Performance	Servidor composto por 16 processadores RISC Power4+ 1.7GHz que apresenta performance mínima de 276.740 SPECjbb2000, com possibilidade de expansão a 553.480 SPECjbb2000	Estão sendo ofertados 16.740 SPECjbb2000 além dos 260.000 SPECjbb2000 mínimos exigidos.	Sim	Manual 25 SPECjbb2000 IBM Corporation IBM eServer pSeries 690 Turbo (págs. 1 e 2) Manual 18 Cálculo para comprovação de Performance (Equipamentos RISC) (pág. 1)

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1000
Doc.

4986

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
2 – Memória RAM	64 Gbytes, instalada, com possibilidade de expansão para, no mínimo, 512 Gbytes, com disponibilidade de recursos para verificação de erro	Mecanismo ECC de detecção e correção de erros	Sim	Manual 22 IBM eServer pSeries 690 (págs. 3, 5 e 6)
3 – Suporte à Arquitetura	SMP – Symetric Multi Processing		Sim	Manual 22 IBM eServer pSeries 690 (págs. 2 e 5)

4 – Fonte de Alimentação	• Estão sendo propostas 2 fontes, número suficiente para suportar a operação do equipamento na configuração máxima especificada:
	  • As fontes possuem recurso de troca sem interrupção (Hot-Swappable/Hot Pluggable)
	  • A alimentação elétrica estará disponível de acordo com a tensão da localidade onde serão instalados os
			Sim	**Manual 23**
				7040-681 IBM (pág. 5)
				Manual 22
				IBM eServer pSeries 690 (pág. 5)3)
				Manual 23
				7040-681 IBM (pág. 20)
				Manual 23
				7040-681 IBM (pág. 5)

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1001
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	equipamentos e a freqüência de alimentação é de 60 (sessenta) Hertz; • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica eum um dos dois (2) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.			**Declaração Comprobatória**
5 – Controladoras e Disco Rígido	• Estão sendo propostas 16 discos de 36GB, com funcionalidade de troca sem interrupção, com tempo médio de acesso menor ou igual a 6ms e com velocidade de rotação mínima de 10.000 RPM. • Estão sendo propostas 8 controladoras de disco PCI		Sim	**Manual 20** **7040-61D IBM (pág. 22)** **Manual 22** **IBM eServer pSeries 690 (pág 3)** **Manual 20** **7040-61D (pág40)**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Doc.
Nº 100

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	Ultra3 SCSI não incorporadas na placa de sistema			
6 – Controladora de I/O	• Estão sendo propostas 16 controladoras Fiber Channel operando a 2Gb/s, para acesso de alta velocidade a unidades de STORAGE e BACKUP. • Estão sendo propostas 16 (dezesseis) interfaces de rede padrão Ethernet PCI 10/100/1000 Base-T em conformidade com os padrões IEEE 802.3ab e 802.3u, com possibilidade de gerenciamento SNMP. • As interfaces de rede irão conectar os servidores a Rede do CCD utilizando cabeamento UTP CAT-6 e conectores RJ-45.		Sim	**Manual 20** **7040-61D IBM (pág. 43)** **Manual 17** **Instalation and Using Guide (pág 1)** **Manual 19** **IBM AIX 5L Operating System (pág. 3)** **Declaração Comprobatória**
7 – Unidade de CD/DVD-ROM e Backup	• Está sendo proposta 1 (uma) unidade de CD-ROM e 1 (uma) unidade de leitora/gravadora de Fita DAT DDS-4		Sim	Manual 23 7040-681 IBM (págs. 40 e 55) Declaração Comprobatória

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• O Servidor possui capacidade de remanejar a unidade de fita e a unidade de CD-ROM para qualquer uma das partições implementadas, pela simples configuração de software, sem a interrupção das aplicações em execução. • A unidade de CD-ROM possui velocidade de 32x. A unidade leitora/gravadora de fita atende ao padrão DDS 4 • Está prevista a entrega de 10 (dez) fitas novas, padrão DDS 3 e 2 (duas) fitas para limpeza para cada unidade leitora/gravadora de fitas			Manual 24 5765-E62 IBM(pág. 2) Manual 23 7040-681 IBM (págs. 40 e 55)
8 – Ambiente Operacional	• Os servidores RISC Tipo 1 estão sendo fornecidos com o seguinte ambiente operacional, licenciado para cada uma das 8 (oito) partições do equipamento: • Sistema operacional AIX 5.2, 64 Bits, instalado e configurado para Rede dos		Sim	Manual 24 5765-E62 IBM(pág. 1)

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1004
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	Correios, com número ilimitado de usuários simultâneos; • Sistema de arquivos JFS (Journaled File System) proposto está disponível dentro do sistema operacional AIX 5.2 • Está sendo proposto o Network Install Manager incluído no sistema operacional AIX 5.2. Esta ferramenta permite o backup e restore do sistema operacional (IMAGE BACKUP) pela rede TCP/IP • Está sendo proposta uma licença do agente "Concord SystemEdge" devidamente instalado e configurado conforme orientação da equipe técnica dos Correios; • Está sendo proposta uma licença de software agente de backup que permite backup LAN FREE compatível com o gerenciador de fitoteca especificado no subitem 5.13			Manual 14 System User's Guide: Operating System and Devices (pág. 54) Manual 15 Installation Guide and Reference (pág. 167) Manual 43 – IBM Tivoli Storage Manager for AIX Storage Agent User's Guide

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0057
Doc. 3668

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	especificado no subitem 5.13 devidamente instalado e configurado conforme orientação da equipe técnica dos Correios. • O sistema operacional AIX 5.2 e o servidor p690 (7040-681) são produzidos pelo mesmo Fabricante – IBM; • Estão sendo fornecidas licenças do compilador C para 6 (seis) servidores RISC TIPO1. A versão fornecida do compilador está homologada para o AIX 5.2. As licenças foram dimensionadas considerando-se o número de processadores fornecidos em cada equipamento. O compilador C é compatível com o padrão ANSI C. • Estão sendo fornecidas e instaladas as licenças do software HACMP 4.5 que permite a criação do ambiente clusterizado entre			(pág.1) Manual "VisualAgeForCAIX.PDF" Pág. 1 e 2 Manual 16 5765-E54 IBM (pág. 1)

ECT - DR/SP
ROS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1006
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	os equipamentos fornecidos. • Estão sendo fornecidas 11 (onze) licenças de HACMP (uma por máquina), que permitem a formação de 16 clusters por equipamento. Essas licenças permitem a criação de até 88 clusters para o ambiente. Dessa forma a ECT pode configurar os seguintes ambientes: • 14 (quatorze) clusters com 2 (dois) nós para o CCD de Brasília/DF; • 6 (seis) clusters com 2 (dois) nós para o CCD de São Paulo/SP			Declaração Comprobatória

5. UNIDADE DE BACKUP

MARCA: IBM

MODELO: 3584-L32

FABRICANTE: IBM

ECT Nº 0007 Doc. 3600 RQS nº 03/2005 - CN CPMI - CORREIOS

Itautec

OBJETIVO
Backup Corporativo

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – Descrição	• Serão fornecidos 2 (dois) sistemas automatizados de armazenamento de dados em cartuchos padrão `LTO Ultrium 2`, incorporando controladora robotizada, gabinete e software de gerenciamento. Sendo 1(um) sistema para o CCD de Brasília-DF e 1 (um) sistema para o CCD de São Paulo-SP		Sim	Manual 5 - SPEC SHEET pag. 01 Manual 6 pag.165 e 172
2 – Capacidade da Biblioteca	• Para o CCD de Brasília, o equipamento possui capacidade de armazenamento e recuperação de dados para a tecnologia'LTO ULTRIUM 2' de, com 60 TB (sessenta Terabytes), sem compressão (nativo); • Para o CCD de São Paulo, o equipamento possui capacidade de armazenamento e recuperação de dados para a tecnologia'LTO		Sim	Manual 5 - SPEC SHEET pag. 01 e 02 Manual 6 pag.195 Manual 5 - SPEC SHEET pag. 01 e 02 Manual 6 pag.195

RQS nº 03/2005 - CN - CPMI - CORREIOS
Doc. Nº 1008

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	ULTRIUM 2' de, com 40 TB (quarenta Terabytes), sem compressão (nativo); • Não será considerada para efeito de cálculo da capacidade solicitada tecnologia de compactação e/ou compressão.			
3 – Capacidade dos Cartuchos	• O Cartucho 'LTO Ultrium 2' possui capacidade de 200 GBytes (sem compressão).		Sim	Manual 5 - SPEC SHEET pag. 01
4 – Compatibilidade	• O hardware é compatível com o padrão 'LTO Ultrium', permiti a leitura de cartuchos, neste padrão, instalados na fitoteca atualmente instalada nos Correios ('3583-L72 IBM LTO Ultrium').		Sim	Manual 5 - SPEC SHEET pag. 01
5 – Quantidade de SLOTS	• Na fitoteca ofertada para o CCD de Brasília possui 300 Slots (60 TB/ 200GB) • Na fitoteca ofetada para o CCD de São Paulo possui 200 Slots (40TB/ 200GB)		Sim	Manual 5 - SPEC SHEET pag. 02 Manual 6 pag.195 Manual 5 - SPEC SHEET pag. 02 Manual 6 pag.195
6 – Quantidade de Cartuchos	• Para o CCD de Brasília está sendo fornecido 600 cartuchos (300*2)		Sim	Proposta Econômica Pág.214

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1000
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• Para o CCD de São Paulo está sendo fornecido 400 cartuchos (200*2)			Proposta Econômica Pág.226
7 – THROUGHPUT por drive	• Os drives apresentam performance nominal de 35MB/segundo para gravação, sem compactação, utilizando cartuchos padrão 'LTO Ultrium 2'		Sim	Manual 5 - SPEC SHEET pag. 01 e 02
8 – Número de DRIVES	• Para o CCD de Brasília, o equipamento possui no 20 (vinte) drives, atingindo o THROUGHPUT nominal de 600 (seiscentos) MB/segundo, utilizando tecnologia de gravação linear, que permite operação simultânea de todos os drives. • Para o CCD de São Paulo, o equipamento possui no 12 (Doze) drives, atingindo o THROUGHPUT nominal de 360 (Trezentos e sessenta) MB/segundo, utilizando tecnologia de gravação linear, que permite operação simultânea de todos os drives.		Sim	Manual 5 - SPEC SHEET pag. 01 e 02 + Proposta Econômica Pág.214 Manual 5 - SPEC SHEET pag. 01 e 02 + Proposta Econômica Pág.226

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1010
Doc.

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
9 – Conectividade	• Fibre Channel, operando a 2 Gbit/sec, entre os servidores e a unidade de backup.		Sim	Manual 5 - SPEC SHEET pag. 01
10 – Recursos de Hardware	• Possui capacidade de manutenção/substituição de cartuchos, sem interrupção dos processos de BACKUP ou RESTORE em curso; • Possui 1 (uma) porta de Comunicação para diagnóstico. • Sistema de leitura de cógido de barras; • Os rótulos dos cartuchos - LABEL, deverão seguir padrão definido pela ECT.		Sim	Manual 6 pag. 162 Manual 6 pag. 180 Manual 6 - pag 22
11 – Retirada das Fitas	• Os equipamentos e Softwares fornecidos permiti a realização da cópia dos dados armazenados nos cartuchos em cartuchos novos.; • Os equipamentos e softwares fornecidos permite que a CONTRATANTE realize a retirada dos cartuchos duplicados sem que esta operação interrompa os demais		Sim	Manual 11 pag. 187 e 198 Manual 11 pag. 145 e 146

ECT CPMI - CORREIOS Doc. Fls Nº 1011 RQS nº 03/2005 - CN

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	porcessos de BACKUP ou RESTORE em curso.			
12 – Recursos Necessários	• O equipamento possui recurso automático para limpeza de todos os drives, utilizando processo transparente de operação; • Será fornecida 1(uma) fita de limpeza para cada drive de leitura/gravação.		Sim	Manual 6 - pag. 25 Proposta Econômica Pág.214 e 226
13 – Recursos de Software	• Serão fornecidas e instaladas nos servidores descritos no subitem 5.15, licenças de software que desempenhe as funções de um GERENCIADOR DE FITA E DE BACKUP;		Sim	• IBM Tivoli Storage Manager for Databases, Data Protection for Oracle for Unix Installation and User's Guide, página VII. • Manual 11 – Pág.3 • Proposta Técnica – pág 24 (Serviço de Implementação de Ambiente pSeries Regatta, Storage e Backup

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1012
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
				– Etapa 05 e 06).
	• As licenças serão fornecidas considerando-se o número de unidades de backup solicitadas e o número total de servidores fornecidos;			Proposta Econômica Pág. 214 e 226
	• Os PRODUTOS de backup fornecidos realizam o BACKUP On-Line do SGBD ORACLE que será instalado em, pelo menos, 10 (dez) partições dos servidores RISC Tipo 01;			Manual 12 Pag.vii IBM Tivoli Storage Manager for Databases, Data Protection for Oracle for Unix Installation and User's Guide, página VII
	• Os PRODUTOS de backup fornecidos realizam o Backup/Restore da base de dados do MS Exchange Server 2000 que será instalado em, pelo menos, 8 (oito) Servidores INTEL Tipo 01.			Manual 13 Pag.vii IBM Tivoli Storage Manager for Mail, Data Protection for Microsoft Exchange Server Installation and User's Guide, pg.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 1078 Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
				VII
14 – Fonte de Alimentação Interna	• O n. de fontes instaladas é suficiente para suportar a operação do equipamento na configuração máxima especificada; • Possui alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme subitem 2.5, freqüência de 60 (sessenta) Hertz; • As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações;		Sim	Manual 6 pag. 192 Manual 5 pag. 2 Manual 6 pag. 192 Manual 5 pag. 1 e 2 Manual 6 pag.191
15 – Geral	• Serão fornecidos 2 (dois) servidores RISC para o CCD de Brasília, em alta disponibilidade, para abrigar os		Sim	Proposta Econômica pág.212

RQS nº 03/2005 - CN - CORREIOS
Fls. Nº 1011
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	softwares gerenciadores das fitotecas e os softwares gerenciadores do backup; • Serão fornecidos 2 (dois) servidores RISC para o CCD de São Paulo, em alta disponibilidade, para abrigar o software gerenciador da fitoteca e o software gerenciador do backup; • Os servidores estarão dimensionados de tal forma que suportem o gerenciamento de, no mínimo, 150 clientes de backup, individualmente.			Proposta Econômica pág.222-223 Declaração Comprobatória

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1013
Doc.

Itautec

6. AMBIENTE DE SEGURANÇA

6.1. SERVIDOR DE SEGURANÇA LÓGICA TIPO 1

MARCA: CISCO

MODELO: PIX-535

FABRICANTE: CISCO

OBJETIVO
Ambiente de Segurança dos CCDs

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento(Sim / Não)**	**Página da documentação Técnica**
1 – Descrição	• Os Servidores de segurança lógica irão operar como firewall, sendo formado por 2 pares de máquinas para cada CCD (Brasília e São Paulo) trabalhando em alta disponibilidade; • O produto tem controle de acesso, permitindo-se atender a uma política de segurança, definindo o		Sim	Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco Pag.2 – Segurança Tipo1 doc1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0916
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	tipo de tráfego que pode entrar/sair das redes protegidas por ele.			
2 – Características e funcionalidades	• Além de Controle de Acesso, o produto provê as seguintes funcionalidades e características: ▪ Autenticação; ▪ Network Address Translation (NAT 1-1 e NAT 1-n); ▪ Segurança de Conteúdo (antivírus, checagem de URL e Java/ActiveX); ▪ Auditoria; ▪ Garantia de disponibilidade no caso de falhas, uma segunda máquina (ou módulo) deve assumir o controle de forma não perceptível aos usuários (stateful firewall failover);		Sim	Pag. 4 – Segurança_Tipo1_doc1 Pag. 4 – Segurança_Tipo1_doc1 Pag. 3 – Segurança_Tipo1_doc1 Pag. 4 – Segurança_Tipo1_doc1 Pag. 3 – Segurança_Tipo1_doc1 Pag. 2 – Segurança_Tipo1_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1001
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ Gerar alertas em tempo real por meio de e-mail quando se tentar violar a política de segurança;			Pag. 2 – Segurança_Tipo1_doc4 Pag. 4 e 13 – Segurança_Tipo1_doc9
	▪ Proteção baseada no algoritmo de segurança adaptável (ASA-Adaptive Secure Algorithm), ou compatível, que oferece um firewall orientado à conexão com classificação;			Pag. 3 – Segurança_Tipo1_doc1
	▪ Prevenção contra ataques de negação de serviço;			Pag. 2 – Segurança_Tipo1_doc1
	▪ Suporte a aplicações multimídia;			Pag. 2 – Segurança_Tipo1_doc1
	▪ Suporte à gerência de Listas de Acesso em Roteadores;			Pag. 33 – Segurança_Tipo1_doc6 Pag. 43 – Segurança_Tipo1_doc6 Pag. 78 – Segurança_Tipo1_doc6 Pag. 2 – Segurança_Tipo1_doc9

ECT - CORREIOS
SCS nº 03/2005 - CN
Fls. Nº 1078
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ Configuração e gerência centralizada em cada um dos sites; ▪ Capacidade de gerenciamento remoto.			Pag. 2 – Segurança_Tipo1_doc3 Pag. 2 – Segurança_Tipo1_doc3
	• O suporte a serviços é estendido a todo e qualquer serviço que funcione sobre protocolo IP, com a possibilidade de customização.			Pag. 21 e 23 – Segurança_Tipo1_doc7 Pag. 1 – Segurança_Tipo1_doc8
	• A interface permitire a visualização da política de segurança definida, com a opção de ocultar e visualizar grupos de regras desejados, e o diagrama da rede protegida.			Pag. 6 e 15 – Segurança_Tipo1_doc5
	• Capacidade de gerar relatórios gerenciais, com informações sobre estatísticas de tráfego,			Pag. 2 – Segurança_Tipo1_doc4

RDS nº 012006 - CN - CPMI - CORREIOS
Fls Nº 1011
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	regras mais utilizadas, entre outras informações. • A solução suporta a integração com outros produtos complementares, tais como: ▪ Sistemas de inspeção de conteúdo (http, FTP, SMTP) de terceiros; ▪ o Suporte ao protocolo H.323. • O produto se integrará perfeitamente com o Sistema para Detecção de Intrusão oferecido. • O produto suporta autenticação de usuário, autenticação de sessão e autenticação de cliente, bem como interagir com os seguintes sistemas de autenticação: ▪ RADIUS; ▪ TACACS. • O sistema de gerenciamento do ambiente de Firewall será disponibilizado pela Itautec em			Pag. 3 e 4 – Segurança_Tipo1_doc1 Pag. 3 – Segurança_Tipo1_doc1 Pag. 3 – Segurança_Tipo1_doc2 Pag. 4 – Segurança_Tipo1_doc1 Pag. 1 – Segurança_Tipo1_doc3

ROS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 1030 Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	hardware à parte, sendo 01 (um) sistema para o CCD de Brasília-DF e 01 (um) sistema para o CCD de São Paulo-SP, podendo estar integrado em um mesmo framework de gerenciamento dos servidores para Detecção de Intrusão, Switch Tipo 06 e Roteador Tipo 01.			Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco
3 – Características de Desempenho	• A configuração do produto apresentará as seguintes características mínimas de desempenho: ▪ Capacidade de tratar no mínimo 400.000 conexões simultâneas; ▪ Possui capacidade de processamento superior a 1.5Gbps, em texto claro.		Sim	Pag. 6 – Segurança_Tipo1_doc1 Pag. 6 – Segurança_Tipo1_doc1
4 – Configuração Física do Equipamento	• Em caso de fornecimento de pares de equipamentos externos ao SWITCH TIPO 1, estes possuirão no mínimo 6 (seis) interfaces 10/100BaseTX, e 2 (duas) interfaces 1000BaseSX.		Sim	Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 1021
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
5 – Características Adicionais	• Todo o ambiente de firewalls será acompanhado de documentação de instalação e configuração. • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz.		Sim	Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco Pag. 7 – Segurança_Tipo1_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1072
Doc.

6.2. SERVIDOR DE SEGURANÇA LÓGICA TIPO 02

Itautec

MARCA: CISCO

MODELO: PIX-525

FABRICANTE: CISCO

OBJETIVO
Ambiente de Segurança dos CCDs - Internet

Requisito	**Atributos Ofertados**	**Atributos Ofertados adicionalmente**	**Confirma Atendimento(Sim / Não)**	**Página da documentação Técnica**
1 – Descrição	• Os Servidores de segurança lógica irão operar como firewall, devendo ser formado por pares de máquinas, com cada par trabalhando em conjunto, com o objetivo de manter a alta disponibilidade do sistema: ▪ 01 (um) par será instalado no CCD de Brasília-DF e 01 (um) par será instalado no CCD de São Paulo-SP. • O produto oferece controle de acesso, permitirá atender a uma política de segurança, definindo o tipo de tráfego que pode entrar/sair das redes protegidas		Sim	Proposta Econômica Pág.217 e 228 Declaração do Fabricante - Cisco Pag. 2 – Segurança_Tipo2_doc1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	por ele.			
2 – Características e Funcionalidades	• Além de Controle de Acesso, o produto deve prover as seguintes funcionalidades e características: ▪ Autenticação;		Sim	Pag. 4 – Segurança_Tipo2_doc1
	▪ Network Address Translation (NAT 1-1 e NAT 1-n);			Pag. 4 – Segurança_Tipo2_doc1
	▪ Segurança de Conteúdo (antivírus, checagem de URL e Java/ActiveX);			Pag. 3 – Segurança_Tipo2_doc1 Pag. 4 – Segurança_Tipo2_doc1
	▪ Auditoria;			Pag. 3 – Segurança_Tipo2_doc1
	▪ Gerenciamento Corporativo, permitirá que vários equipamentos sejam gerenciados a partir de uma única console;			Pag. 1 – Segurança_Tipo2_doc5

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1021
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ Garantia de disponibilidade. No caso de falhas, uma segunda máquina (ou módulo) deve assumir o controle de forma não perceptível aos usuários (stateful firewall failover);			Pag. 2 – Segurança_Tipo2_doc1
	▪ Gerar alertas em tempo real por meio de e-mail quando se tentar violar a política de segurança;			Pag. 2 – Segurança_Tipo2_doc5 Pag. 4 e 13 – Segurança_Tipo2_doc11
	▪ Proteção baseada no algoritmo de segurança adaptável (ASA-Adaptive Secure Algorithm), ou compatível, que oferece um firewall orientado à conexão com classificação;			Pag. 3 – Segurança_Tipo2_doc1
	▪ Prevenção contra ataques de negação de serviço;			Pag. 2 – Segurança_Tipo2_doc1
	▪ Suporte a aplicações multimídia;			Pag. 2 – Segurança_Tipo2_doc1
	▪ Suporte à gerência de Listas de			Pag. 33 – Segurança_Tipo2_doc8

Doc. 2201 Fls. Nº
CPMI - CORREIOS
RQS nº 03/2005 - CN

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	Acesso em Roteadores;			Pag. 43 – Segurança_Tipo2_doc8 Pag. 78 – Segurança_Tipo2_doc8 Pag. 2 – Segurança_Tipo2_doc11
	▪ Configuração e gerência centralizada em cada um dos sites;			Pag. 1 – Segurança_Tipo2_doc4
	▪ Capacidade de gerenciamento remoto.			Pag. 2 – Segurança_Tipo2_doc4
	• O suporte a serviços deve ser estendido a todo e qualquer serviço que funcione sobre protocolo IP, com a possibilidade de customização.			Pag. 21 e 23 – Segurança_Tipo2_doc9 Pag. 1 – Segurança_Tipo2_doc10

RDS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 1090
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• A interface permite a visualização da política de segurança definida, com a opção de ocultar e visualizar grupos de regras desejados, e o diagrama da rede protegida.			Pag.6 e 15 – Segurança_Tipo2_doc7
	• Capacidade de gerar relatórios gerenciais, com informações sobre estatísticas de tráfego, regras mais utilizadas, entre outras informações.			Pag. 2 – Segurança_Tipo2_doc5
	• A solução tem que suportar a integração com outros produtos complementares, tais como: ▪ Sistemas de inspeção de conteúdo (HTTP, FTP, SMTP) de terceiros;			Pag. 3 e 4– Segurança_Tipo2_doc1 Pag. 4 – Segurança_Tipo2_doc1
	▪ Suporte ao protocolo H.323.			Pag. 3 – Segurança_Tipo2_doc2

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	• O produto se integrará perfeitamente com o Sistema para Detecção de Intrusão oferecido.			Pag.4 – Segurança_Tipo2_doc1
	• O produto tem que suportar autenticação de usuário, autenticação de sessão e autenticação de cliente, bem como interagir com os seguintes sistemas de autenticação: ▪ RADIUS; ▪ TACACS.			Pag.1 – Segurança_Tipo2_doc3
	• O produto suportará VPN padrão IPSEC, com as seguintes características: ▪ Algoritmos de criptografia (DES, 3DES);			Pag.2 – Segurança_Tipo2_doc3
	▪ Capacidade superior a 1000 conexões simultâneas;			Pag.2 – Segurança_Tipo2_doc3
				Pag.2 –

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1092
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	▪ Capacidade de processamento em 3DES superior a 50Mbps; ▪ Suporte a certificados digitais X.509v3. O sistema de gerenciamento do ambiente de Firewalls será disponibilizado pela Itautec no mesmo hardware gerenciador dos SERVIDORES DE SEGURANÇA LÓGICA TIPO01 , sendo 01 (um) sistema para o CCD de Brasília-DF e 01 (um) sistema para o CCD de São Paulo-SP.			Segurança_Tipo2_doc3 Pag. 3 – Segurança_Tipo2_doc6 Pag. 1 – Segurança_Tipo2_doc4 Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco
3 – Características de Desempenho	• A configuração do produto apresentará as seguintes características mínimas de desempenho: ▪ Capacidade de tratar no mínimo 280.000 conexões simultâneas; ▪ Possuirá capacidade de		Sim	Pag. 6 – Segurança_Tipo2_doc1

Doc. 3800
ECT CPMI - CORREIOS
Fls Nº 0279

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	processamento superior a 350Mbps, em texto claro.			Declaração de Fabricante - Cisco
4 – Configuração Física do Equipamento	• Em caso de fornecimento de pares de equipamentos externos ao SWITCH TIPO 1, estes devem possuir no mínimo 6 (seis) interfaces 10/100BaseTX, e 01 (uma) interface 1000BaseSX.		Sim	Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco
5 – Características Adicionais	• Todo o ambiente de firewalls será acompanhado de documentação de instalação e configuração. • Possuirá alimentação elétrica de acordo com a localidade onde instalarão os equipamentos, conforme subitem 2.5., freqüência de 60 (sessenta) Hertz.		Sim	Proposta Econômica Pág.216 e 228 Declaração do Fabricante - Cisco Pag. 7 – Segurança_Tipo2_doc1

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 1000 Doc.

Itautec

6.3. SERVIDOR PARA DETECÇÃO DE INTRUSÃO

MARCA: CISCO

MODELO: IDS-4250

FABRICANTE: CISCO

OBJETIVO
Detecção e Verificação de Ataques à Rede Corporativa dos Correios

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – Descrição	• O SERVIDOR DE DETECÇÃO DE INTRUSÃO irá operar como Intrusion Detection System - IDS, sendo formado por: ▪ 02 (dois) módulos que devem integrar-se ao SWITCH TIPO 1, tomando o tráfego diretamente no painel traseiro desse Switch, sendo que 01 (um) módulo será instalados no CCD de Brasília-DF e 01 (um) módulo será instalado no CCD de São Paulo-SP; ▪ Permitirá a utilização de 02		Sim	Pag. 3 – Intrusão_doc1 Proposta Econômica Pág.217 e 228 .

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 2061
Doc.

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	(dois) equipamentos externos, sendo 01 (um) equipamento no CCD de Brasília- DF e 01 (um) equipamento no CCD de São Paulo-SP, desde que a tomada do tráfego seja realizada através de 1 (uma) das portas SPAN do SWITCH TIPO 01.			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0668
Doc.

2 – Características e Funcionalidades	• O ambiente de IDS é composto por dois elementos complementares: • Sensor: ▪ Responsável por monitorar a rede a que está conectado, analisando tanto o cabeçalho (header) como a área de dados (payload) de cada pacote que trafega pela rede citada, de modo a verificar se os referidos pacotes constituem tráfego autorizado. ▪ O sensor é capaz de monitorar o tráfego de redes TCP/IP, observando no mínimo uma interface de rede com 500 Mbps em tráfego full. ▪ O sensor oferece uma interface de controle 10BaseT/100BaseTX (em caso de equipamento externo ao SWITCH TIPO 1); ▪ O sensor funciona de forma transparente, ou seja, não deve causar impacto no desempenho do switch, monitorando o tráfego no painel traseiro de comutação do switch (em caso de utilização de módulos para o SWITCH		Sim	Pag. 1 – Intrusão_doc5 Pag. 1 – Intrusão_doc4 Pag. 2 e 3 – Intrusão_doc1 Pag. 3 – Intrusão_doc1 Estamos usando solução externa.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1093
Doc.

	TIPO 1); ▪ O sensor possui a capacidade de monitorar diversas VLANs simultaneamente, utilizando o recurso de captura VLAN ACL ou a funcionalidade SPAN. • Software de controle: ▪ o Software baseado em sistema operacional HP-UX, Solaris, AIX, Windows 2000 ou LINUX, capaz de monitorar de forma centralizada a atividade de múltiplos sensores, estejam estes localizados em segmentos de rede locais ou remotos. Deve ser possível configurar remotamente os sensores utilizando se o software de controle. Em caso de falha de um dos sensores utilizados, um alarme deve ser enviado para o software de controle. O software de controle deve registrar em uma base de dados às configurações de cada um dos sensores que lhe são subordinados. A comunicação entre os sensores e o software de controle deve ser autenticada. O			Pag. 3 – Intrusão_doc4 Pag. 7 e 13 – Intrusão_doc11 Pag. 1 – Intrusão_doc5 Pag. 3 – Intrusão_doc11 Pag. 2 – Intrusão_doc5 Pag. 10 – Intrusão_doc12

ECT - CORREIOS - CPMI
Fls. Nº 1608
Doc.

	software de controle permitirá integração com base de dados Oracle versão 8.i ou superior, ou SQL Server versão 2000 ou superior. ▪ O sistema analisa cada um dos pacotes que trafegam pela rede a que está conectado e também a relação de tais pacotes com os adjacentes a ele no fluxo de dados da rede. Imediatamente após a identificação de uma eventual violação da política de segurança o sensor deve enviar um alarme para o software de controle.			Pag. 2 – Intrusão_doc2 Pag. 3 – Intrusão_doc4
	• O bloqueio de uma tentativa de invasão não afeta os demais usuários.			Pag. 5 – Intrusão_doc1
	• O sistema permitirá a detecção das seguintes classes de ataques: ▪ Ataques com nomes específicos: tais como PHF e Smurf;			Pag. 3 – Intrusão_doc2
	▪ Ataques genéricos: (ataques nomeados com múltiplas variações) tais como Pacotes IP fragmentados e Teardrop;			Pag. 3 – Intrusão_doc2

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1037
Doc.

	▪ Ataques que utilizam recursos de detecção Whisker anti-IDS; ▪ Ataques com assinaturas complexas: tais como Simplex-Mode TCP hijacking e E-mail Spam; ▪ Ataques a servidores Web, a servidores de E-mail, "Denial of Service", "FTP exploits", acesso não autorizado, a servidores de banco de dados, a servidores de aplicação e serviço (NT, Solaris, HP-UX, AIX, Linux), a servidores DNS e Probin Attacks. • O sistema ainda permite a criação de regras personalizadas de identificação de invasões para que possa ser adaptado à estrutura particular disponível na ECT . À medida que novos ataques forem sendo descobertos deve ser possível criar "assinaturas"			Declaração de Fabricante - Cisco Pag. 3 – Intrusão_doc2 Pag. 1 a 12 – Intrusão_doc13 Declaração de Fabricante - Cisco Pag. 6 – Intrusão_doc4 Pag. 3 – Intrusão_doc5

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1026
Doc

	associadas aos mesmos de modo a prevenir tentativas de reincidência. • O software de controle é capaz de enviar alarmes via e-mail para notificar a violação de uma dada regra de segurança. • O sistema registra informações tais como origem, destino, horário e tipo dos ataques ocorridos. • O sistema possibilita a atualização automática das "assinaturas" através de download seguro via Web. • O Sistema possui suporte a SSH para comunicação e configuração segura. • O sistema deve realizar a verificação do TCP Three Way Handshake. • Além disso, o sistema: ▪ Oferece respostas em tempo real para os ataques via rede, com			Pag. 2 – Intrusão_doc6 Pag. 2 – Intrusão_doc3 Pag. 7 – Intrusão_doc4 Pag. 2 – Intrusão_doc4 Pag. 5 – Intrusão_doc8

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1093
Doc.

	possibilidade de término da sessão e reconfiguração de regras de acesso em firewall, que seja possível configurar;			Pag. 5 – Intrusão_doc1
	▪ Suporta captura de log de sessão no formato padrão TCP Dump;			
	▪ Bloqueia tentativas de invasão, que seja possível configurar;			Pag. 5 – Intrusão_doc1
	▪ Permite a verificação de decodificação de protocolos, scripts CGI, DNS, acesso remoto via BIND, daemons;			Pag. 2 – Intrusão_doc3
				Pag. 1 a 12– Intrusão_doc13
	▪ Permite a customização de respostas a intrusões, mascaramento de tráfego, criação de conexões e modificação de ações de resposta;			Pag. 5 – Intrusão_doc1
	▪ Possui ferramentas de			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1080
Doc.

	configuração com interface gráfica, controlando múltiplos sistemas de detecção;			
	▪ Registra as sessões de ataques, com possibilidade de "playback";			Pag. 1 – Intrusão_doc5
	▪ Utiliza base de dados em tempo real para ajuda a resposta a incidentes ocorridos;			Pag. 6 – Intrusão_doc4
	▪ Gera sumários de relatórios das atividades registradas;			Pag. 2 – Intrusão_doc6
	▪ Utiliza recurso de e-mail e traps SNMP para envio de informações a consoles com plataforma de gerenciamento;			Pag. 2 – Intrusão_doc5 Pag. 2 – Intrusão_doc5
	▪ Detecta eventos em ambientes computacionais com os sistemas operacionais Windows NT 4.0 (Server e Workstation) e Unix (AIX, Solaris, Linux, HP-UX);			Pag. 2 – Intrusão_doc9

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1088
Doc.

	▪ Fornece suporte ao gerenciamento de riscos através de relatórios técnicos e gerenciais pré-definidos, com detalhamento das informações coletadas; ▪ Permite a criação de relatórios técnicos e gerenciais personalizados, em formas textuais e gráficas; ▪ Possui documentação detalhada para possibilitar a configuração; ▪ É robusto para suportar qualquer tipo de ataque contra si próprio; ▪ Permitirá a instalação sem necessidade de alteração na infraestrutura de rede e sem causar degradação do seu			Pag. 1 – Intrusão_doc4 Pag. 8 – Intrusão_doc4 Pag. 2, 3, 4, 5, 7 – Intrusão_doc10 Pag. 2 – Intrusão_doc6 Serão entregues os manuais do produto que permitem sua configuração Pag. 5 – Intrusão_doc4

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 1001
Doc:

	desempenho; Permite a configuração remota, a partir da console de gerenciamento.			Pag. 7 – Intrusão_doc4 Pag. 1 – Intrusão_doc5
3 – Características Adicionais	• O ambiente de gerenciamento dos Servidores IDS será disponibilizado pela Itautec em hardware exclusivo, à parte, podendo estar integrado em um mesmo framework de gerenciamento dos SERVIDORES DE SEGURANÇA LÓGICA, SWITCH TIPO 5 e ROTEADOR TIPO 1; • Todo o ambiente de será acompanhado de documentação de instalação e configuração; • O produto deve integrar-se, de forma transparente, com o ambiente de gerência dos SERVIDORES DE SEGURANÇA LÓGICA, sendo capaz de reconfigurar automaticamente as regras desses equipamentos.		Sim	Pag. 1 – Intrusão_doc5 Proposta Econômica Pág.217 e 228 Proposta Econômica Pág.217 e 228 Pag. 2 – Intrusão_doc7

RQS nº 03/2005 - C
CPMI - CORREIO
Doc.
Fls 1044

Itautec

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1042
Doc.

Itautec

7. RACK PARA EQUIPAMENTOS

MARCA: IBM

MODELO: 9306-420

FABRICANTE: IBM

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
1 – Estrutura Física	• Todos os equipamentos fornecidos, que não tenham RACK próprio do fabricante, serão instalados em estruturas de RACK, com as seguintes características: ▪ RACK do tipo fechado, em aço, com 19" de largura e profundidade de 103cm, para fixação dos dispositivos ofertados; ▪ Altura de 42U; ▪ Permite a instalação de todos os equipamentos com largura padrão de 19" (dezenove polegadas); ▪ Sistema de ventilação através de portas perfuradas; ▪ colunas de segundo plano		Sim	**Manual 26:** Página Web do componente : - Rack Principal: P/N: 9306-420 – Pag. 65 - Rack Extensor: P/N : 9306-421 – Pag. 67 **Declaração Comprobatória**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1043
Doc.

Itautec

Requisito	Atributos Ofertados	Atributos Ofertados adicionalmente	Confirma Atendimento(Sim / Não)	Página da documentação Técnica
	(aproximadamente 10 cm); ▪ sistema de chave e fechadura; laterais e traseira removíveis; guias de roteamento verticais e horizontais (organizadores de cabos).			

RGB
CPMI - CORREIOS
Fls
Doc.

2 – Estrutura Funcional	• Os RACKS serão interligados à rede elétrica através de tomadas tripolares, a serem instaladas pela Itautec quando realizar a adequação da estrutura elétrica das Salas de Segurança Físicas, conforme subitem 1.3.1. alínea i. do ANEXO 1-A do Edital; • A Itautec instalará 32 (trinta e duas) réguas de tomadas no suíte de Racks no CCD de Brasília, e outras 27 (vinte e sete), no CCD de São Paulo, considerando cada circuito elétrico existente na Sala de Segurança Física, com tomadas universais em número suficiente para total de elementos instalados no RACK. As réguas possuem pinagem compatível com as tomadas dos equipamentos instalados no RACK. • OBS.: As PDUs deverão ter suas tomadas removidas e substituídas por tomadas padrão ABNT.		Sim	**Manual 26:** Página Web do componente : - P/N : 32P1736 – Pag. 77
3 – Gerais	• A quantidade de RACKS dimesionada pela Itautec é de 8 para o CCD de Brasília e 5 para o		Sim	Proposta Econômica conforme Configuração (pág.210) e descrito.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 1045
Doc.

	CCD de São Paulo e deverá ser aprovado pela ECT, levando-se em conta a atual distribuição dos equipamentos nas Salas de Segurança Física e os critérios de padronização do layout definidos pela ECT.			

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1040
Doc.

Itautec

4. Configuração de Equipamentos

4.1 Brasília

SWITCH TIPO 1 e SERVIDOR DE SEGURANÇA LÓGICA TIPO 1

Product	Description	Quantity
WS-C6513	Cat 6513 Chassis, 13slot, 19RU, No Pow Supply, No Fan Tray	1
WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613	1
WS-CAC-2500W	Catalyst 6000 2500W AC Power Supply	1
WS-CAC-2500W/2	Catalyst 6000 Second 2500W AC Power	1
CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL	2
SC6K-S2CVK9-7.6.1	Catalyst 6000 Sup 2 Flash Image w/CV and SSH, Release 7.6.1	1
WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2	1
S6MSF2ZV-12113E	Catalyst 6000 MSFC2 IOS SERVICE PROVIDER W/VIP	1
WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module 2	1
WS-X6516-GBIC	Catalyst 6500 16-port GigE Mod: Fabric-Enabled (Req. GBICs)	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6066-SLB-APC	Catalyst 6000 Content Switching Module	1
SC6K-3.1.3-CSM	CSM 3.1.3 Software Release	1
WS-SVC-NAM-1	Catalyst 6500 Network Analysis Module-1	1
SC-SVC-NAM-3.1	Catalyst 6500 NAM SW Release 3.1	1
WS-SVC-FWM-1-K9	Firewall blade for Catalyst 6500	1
SC-SVC-FWM-1.2-K9	Firewall Module Software 1.1(2) for Catalyst 6500	1
WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	18
MEM-S2-128MB	Catalyst 6000 Sup2 Mem, 128MB DRAM Option	1
MEM-MSFC2-128MB	Catalyst 6000 MSFC-2 Mem, 128MB DRAM Option	1
SF-PIX-PDM-2.1	PIX Device Manager for FW Module for Catalyst 6500	1

SWITCH TIPO 2

Product	Description	Quantity
WS-C2950G-48-EI	Catalyst 2950, 48 10/100 with 2GBIC slots, Enhanced Image	1
CAB-AC	Power Cord,110V	1
WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable	1
CAB-RPS-1614=	1 RPS 675 connector cable 16/14	1
WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	1
WS-C2950T-24	24 10/100 ports w/ 2 10/100/1000BASE-T ports, Enhanced Image	1
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable	1
CAB-RPS-1614=	1 RPS 675 connector cable 16/14	1

RQS nº 03/2005 - C
CPMI - CORREIO
Pág. 207
Fls. Nº 1047
Doc.

Itautec

SWITCH TIPO 3

Product	Description	Quantity
2109-C36	IBM TotalStorage Cabinet C36	1
6080	Ruggedized Rack Feature	1
9200	Quantity of Plant Installed 2109-M12's	2
9751	Brazilian/Portuguese	1
9823	Single Phase Group 2 Cord	1

Product	Description	Quantity
2109-M12	IBM TotalStorage SAN Switch – 128 Port	1
2310	M12 Shortwave SPF Transceiver	128
3216	16port 2Gb Switch Blade	6
5325	M12 Fiber Cable (multimode)	128
7201	Fabric Manager	1
9202	Second M12 Installed in 2109-C36	1

Product	Description	Quantity
2109-M12	IBM TotalStorage SAN Switch - 128 Port	1
2310	M12 Shortwave SPF Transceiver	128
3216	16port 2Gb Switch Blade	6
5325	M12 Fiber Cable (multimode)	128
7201	Fabric Manager	1
9201	First M12 Installed in 2109-C36	1

SWITCH TIPO 4

Product	Description	Quantity
KV138A	CHASSIS AFFINITY ARQUITETURA 8 USUARIOS	14
KV1301C-R2	AFFINITY USER/CPU C 1 X 4 CARD	28
KV1300C	SERVSWITCH AFFINITY - PLACA 0 USER X 4 CPUS	28
KV1306C	SERVSWITCH AFFINITY HI-DENSITY EXPANS	14
RMK19A-BB	SERVSWITCH AFFINITY KIT PARA RACK 19"	14
KV180035	SERVSWITCH AFFINITY HI-DENS EXP CABLE	50
EHN515-0035	CABO SERVSWITCH CPU SUN/HD15 COM 10,6M	28
EHN382-0035	CABO SERVSWITCH CPU COAX PC COM 10,6M	100
EHN382-0100	CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M	100
EHN383-0100	CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M	8
EHN225-0100	CABO SERVSWITCH CONSOLE SUN/HD15 COM 30,0M	8

Monitor, Teclado e Mouse

Product	Description	Quantity
31P7453	Teclado ABNT	8
28L3673	Mouse	8
31P8136	Monitor 17" Preto	8

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 1048
Doc.

Itautec

SWITCH TIPO 5

Product	Description	Quantity
CVPN3060-HA-K9	2 Complete VPN 3060 Redundant Systems	1
CAB-AC	Power Cord,110V	1
CVPN3060-SW-K9	Software for VPN3060 Concentrator	1
CAB-AC	Power Cord,110V	1
CVPN3060-SW-K9	Software for VPN3060 Concentrator	1

ROTEADOR TIPO 1

Product	Description	Quantity
CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router	1
PWR-3745-AC	AC Power Supply for the Cisco 3745	1
PWR-3745-AC/2	Redundant AC System Power Suppy for the Cisco 3745	1
CAB-AC	Power Cord,110V	2
S374AK9-12301	Cisco 3745 Ser IOS ENTERPRISE PLUS IPSEC 3DES	1
NM-1FE2W	1 10/100 Ethernet 2 WAN Card Slot Network Module	1
WIC-2T	2-PORT SERIAL WAN INTERFACE CARD	2
NM-1A-E3	1-PORT E3 ATM NETWORK MODULE	2
NM-1GE	1 Port GE Network Module	1
WIC-2T	2-PORT SERIAL WAN INTERFACE CARD	2
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	8
WS-G5483=	1000BASE-T GBIC	1

ROTEADOR TIPO 2

Product	Description	Quantity
CISCO1751-V	10/100 Modular Router w/Voice,32F/64D	1
MEM1700-64U96D	Cisco 1751-V 64MB to 96MB DRAM Factory Upgrade	1
S17C7VK9-12215T	Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 3DES	1
WIC-2T	2-PORT SERIAL WAN INTERFACE CARD	1
VIC-2FXO	Two-port Voice Interface Card - FXO	1
VIC-2FXS	Two-port Voice Interface Card - FXS	1
PVDM-256K-4	4-CHANNEL PACKET VOICE/FAX DSP MODULE	1
CAB-AC	Power Cord,110V	1
CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet	1
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	1
PVDM-256K-4	4-CHANNEL PACKET VOICE/FAX DSP MODULE	1
ROUTER-SDM	Device manager for routers	1
PVDM-256K-4	4-CHANNEL PACKET VOICE/FAX DSP MODULE	1

ROS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 209
Fls. Nº 1049
Doc:

Itautec

INTEL TIPO 1 (x440)

Product	Description	Quantity
8687-7RX-LM	x440 Xeon MP 2.0GHz/2MB L3 (4way), 2GB	14
59P5188	SMP Expansion Module	14
59P5173	Xeon MP 2.0GHz/2MB L3 proc. upgr.	56
33L3324	512MB PC133 ECC SDRAM RDIMM	168
06P5756	73.4GB 10K U160 SCSI HS HDD	28
06P5740	4Lx	14
24P0960	FC2-133 Host PCI Adapter	28
31P6301	NetXtreme 1000T Ethernet PCI Adapter	42

INTEL TIPO 2 (x360)

Product	Description	Quantity
8686-9RX-LM	x360 Xeon MP 2.0GHz/2MB L3 (2way), 2GB	29
59P6817	Xeon MP 2.0GHz/2MB L3 proc. upgr.	58
33L3283	512MB PC1600 ECC DDR SDRAM RDIMM	116
06P5756	73.4GB 10K U160 SCSI HS HDD	58
06P5740	4Lx	29
24P0960	FC2-133 Host PCI Adapter	58
31P6301	NetXtreme 1000T Ethernet PCI Adapter	58
31P6108	370W HS Redundant PS	29

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	27
02R1988	Xeon 3.06GHz/512KB proc. upgr.	27
33L5038	512MB DDR PC2100 ECC RDIMM	54
32P0727	73.4GB 10K U320 SCSI HS HDD	54
31P6301	NetXtreme 1000T Ethernet PCI Adapter	54
59P4211	5U x 24D Tower-to-Rack Kit III	27

RACK

Product	Description	Quantity
9306-420	NB42SR	1
9306-421	NB42SX	7
32P1736	DPI Universal Rack PDU	32
94G6670	Blank Filler Panel Kit	6
94G7448	IEC 320 C14	64

DGS 03/2005 CN
CPMF CORREIOS
Fls. Nº 1010
Doc.

Itautec

9843

INTEL ADICIONAIS

INTEL TIPO 2 (x360)

Product	Description	Quantity
8686-9RX-LM	x360 Xeon MP 2.0GHz/2MB L3 (2way), 2GB	1
59P6817	Xeon MP 2.0GHz/2MB L3 proc. upgr.	2
33L3283	512MB PC1600 ECC DDR SDRAM RDIMM	4
06P5756	73.4GB 10K U160 SCSI HS HDD	2
06P5740	4Lx	1
24P0960	FC2-133 Host PCI Adapter	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	2
31P6108	370W HS Redundant PS	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
24P0960	FC2-133 Host PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity

REG nº 03/2005 - CP
ECT CORREIOS
Fls. Nº
Doc.

Itautec

8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

RISC TIPO 1

Product	Description	Quantity
7040-681	Rack Server 1:pSeries 690 Model 681 CEC	8
2624	32X (Max) SCSI-2 CD-ROM Drive	8
3155	Diskette Drive Cable	8
3255	Operator Panel Attachment Cable	8
4199	128MB Level 3 Cache (4 x 32MB), 567MHz	16
4484	16GB Memory Card, 567MHz, Inward Facing	32
4618	Drawer Placement Indicator, 18U Position, Primary Rack	8
4651	Rack Indicator, Rack #1	8
5246	8-Way POWER4+ Turbo Processor Option	16
5251	Processor Clock Card, Programmable	8
5257	Processor Bus Pass Through Module	16
6158	20/40GB 4mm Internal Tape Drive	8
6161	Cable Group, Power Controller to CEC and Fans	8
6162	Interface Cable, Service Processor to Power Subsystem	8
6170	Power Converter Assembly, Central Electronics Complex	16
6181	Power Cable Group, CEC to Power Controller	8
6182	Power Cable Group, CEC to Power Controller	8
6183	Power Cable Group, CEC to Power Controller	8
6189	DC Power Converter, CEC, Additional	16
6198	Capacitor Book, Two Processor Modules	8
6418	Support Processor with Remote I/O-2 (RIO-2) Loop Attachment, Two Loops	8
6419	Remote I/O-2 (RIO-2) Loop Adapter, Four Loop	8
6565	Backplane, Central Electronics Complex	8
8121	Attachment Cable, Hardware Management Console to Host, 15-Meter	8
8692	Media Drawer, Operator Panel, Diskette	8
9300	Language Group - US English	8

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1053
Doc.

0841

Itautec

Product	Description	Quantity
7040-61D	I/O Drawer 1:Model 61D I/O Drawer	8
2118	Converter Cable, VHDCI to P, Mini-68 pin to 68 pin, 0.3M	8
2122	SCSI Cable - I/O Drawer to Media Drawer	8
2943	8-Port Async Adapter EIA-232/RS-422 (PCI)	16
3125	Serial to Serial Port Cable for Rack/Rack	16
3156	RIO-2 (Remote I/O-2) Cable, 1.75M	32
3277	36.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly	64
4609	Drawer Placement Indicator, 9U Position, Primary Rack	8
4651	Rack Indicator, Rack #1	8
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	64
6121	I/O Drawer Attachment Cable Group, Drawer Position #4609	8
6172	Power Converter Assembly, I/O Drawer	16
6179	Power Cable, I/O Drawer to Media Drawer	8
6203	PCI Dual Channel Ultra3 SCSI Adapter	8
6239	2 Gigabit Fibre Channel PCI-X Adapter	64
6564	Ultra3 SCSI 4-Pack Hot Swap Back Plane	32
6571	I/O Drawer PCI-X Planar, 10 Slot, 2 Integrated Ultra3 SCSI Ports	16
9300	Language Group - US English	8

Product	Description	Quantity
7040-61D	I/O Drawer 2:Model 61D I/O Drawer	8
2118	Converter Cable, VHDCI to P, Mini-68 pin to 68 pin, 0.3M	8
2943	8-Port Async Adapter EIA-232/RS-422 (PCI)	16
3125	Serial to Serial Port Cable for Rack/Rack	16
3156	RIO-2 (Remote I/O-2) Cable, 1.75M	32
3277	36.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly	64
4605	Drawer Placement Indicator, 5U Position, Primary Rack	8
4651	Rack Indicator, Rack #1	8
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	64
6122	I/O Drawer Attachment Cable Group, Drawer Position #4605	8
6172	Power Converter Assembly, I/O Drawer	16
6203	PCI Dual Channel Ultra3 SCSI Adapter	8
6239	2 Gigabit Fibre Channel PCI-X Adapter	64
6564	Ultra3 SCSI 4-Pack Hot Swap Back Plane	32
6571	I/O Drawer PCI-X Planar, 10 Slot, 2 Integrated Ultra3 SCSI Ports	16
9300	Language Group - US English	8

Product	Description	Quantity
7040-61R	7040-61R : Rack 1:Model 61R Rack	8
0190	Rack Content: 7040/681 – 17U	8
0191	Rack Content: 7040/61D – 4U	16
0192	Rack Cont: 7040/681 8692 – 1U	8
0193	Rack Cont: 7040/61R 8690 – 8U	8
4651	Rack Indicator, Rack #1	8
6070	Front Door, Black with Copper Accent, Primary Rack	8
6075	Rear Door, Acoustic, Primary or Secondary Rack	8
6186	Bulk Power Regulator	32
6187	Power Controller, Four Cooling Fans, Three DC Power Converter	16

ROS nº 03/2005 - CN
CPMI - CORREIOS
Pag. 213
Fls. Nº 1052
Doc.

Itautec

	Connections	
6188	Power Distribution Assembly	16
8678	Line Cord, 6AWG, 14ft, IEC309 Plug	16
8690	Bulk Power Assembly, Redundant	8
9300	Language Group – US English	8

Product	Description	Quantity
7315-C02	HMC 1:Hardware Management Console	2
0966	pSeries Indicator	2
2943	8-Port Async Adapter EIA-232/RS-422 (PCI)	2
3627	IBM P76/P77 Color Monitor, Stealth Black, Captured Cable	2
4962	10/100 Mbps Ethernet PCI Adapter II	2
5005	Software Preinstall (RS)	2
8121	Attachment Cable, Hardware Management Console to Host, 15-Meter	16
8800	Quiet Touch Keyboard - USB, Stealth Black, US English, #103P	2
8841	Mouse - Stealth Black with Keyboard Attachment Cable	2
9004	Southern Hemisphere Designator for Monitors	2
9300	Lang Grp Spec.-US Eng.	2
9800	Power Cord Specify - US/Canada	2

Notebook – console para RISC TIPO 1

Product	Description	Quantity
2388-BP2	Notebook IBM ThinkPad G40	4

UNIDADE DE BACKUP

Product	Description	Quantity
3584-D32	IBM UltraScalable Tape Library Expansion Frame	1
1452	Frame Control Assembly	1
1462	Fibre Channel Patch Panel	1
1476	LTO Ultrium 2 Fibre Drive Canister	8
1660	10/100 Ethernet Support	1
1901	Dual AC Power	1
1902	Additional AC Power	2
6025	25M LC-LC Fibre Channel Cable	1
9212	Attached to Windows System	1
9600	Attached to RS/6000	1

Product	Description	Quantity
3584-L32	IBM UltraScalable Tape Library	1
1462	Fibre Channel Patch Panel	1
1476	LTO Ultrium 2 Fibre Drive Canister	12
1603	Capacity Expansion	1
1662	3584 Specialist	1
1901	Dual AC Power	1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 214
Fls. Nº 1105
Doc.

2710	Remote Support Facility	1
6025	25M LC-LC Fibre Channel Cable	56
9002	First Expansion Frame Attachment	1
9212	Attached to Windows System	1
9600	Attached to RS/6000	1
9660	10/100 Ethernet Support	1

Product	Description	Quantity
3589-004	Ultrium cleaning cartridges	1
4005	5-pack Ultrium cleaning cartridge	4

Product	Description	Quantity
3589-006	200GB Ultrium Tape Cartridges with Labeling Services	1
6020	200GB Ultrium Tape Cartridges w/Label 20-pack	30
8000	Jewel Cases	1
9006	Label background color Lt Blue	1
9022	Color/vibrant background	1
9110	First character of Volser is A	1
9200	Second character of Volser is 0	1
9300	Third character of Volser is 0	1
9400	Fourth character of Volser is 0	1
9500	Fifth character of Volser is 0	1

Disco SSA (576GB) para Ambiente de Alta Disponibilidade ITSM - Backup

Product	Description	Quantity
7133-D40	7133-D40 SERIAL DISK SYSTEM -ADVANCED Drawer Model	1
0550	0550 Havant Mfg. Indicator	1
8022	8022 50/60 HZ AC Power Supplies	1
8031	8031 Raven Black Drawer Cover	1
8399	8399 Additional Dummy Drive	8
8572	8572 Advanced 10K rpm/72.8 GB Disk Module	8
8802	8802 2.5 Meter Advanced SSA Cable	4
9300	9300 Language Groups - US English	1

ITSM – BACKUP (RISC ADICIONAL)

Dois servidores Risc em alta disponibilidade e Rack

Product	Description	Quantity
7028-6C4	ITSM SPM:pSeries 630 Model 6C4 Rack-mount Server	2
2633	CD-ROM Drive - 48X (Max) IDE	2
2848	POWER GXT135P Graphics Accelerator	2
3158	36.4 GB 10,000 RPM Ultra3 SCSI Disk Drive Assembly	4
3254	RIO Cable Support Brackets	2
4250	Connector Cable, 6-slot PCI Riser to Media Bays.	2
4254	SCSI Connector Cable	2
4452	2048MB (4x512MB) SDRAM DIMM Memory	4
4651	Rack Indicator, Rack #1	2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1055
Doc.

0838

Itautec

5127	2-way 1.45 GHz POWER4+ Processor Card	4
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6158	20/40GB 4mm Internal Tape Drive	2
6230	Advanced SerialRAID Plus Adapter	2
6239	2 Gigabit Fibre Channel PCI-X Adapter	6
6273	Power Supply ,645 Watt AC, Hot-Swap, Base and Redundant	4
6557	Redundant Cooling	2
6568	Ultra3 SCSI 4-Pack Hot Swap Back Plane	2
9172	Power Specify, AC	2
9300	Lang.Group Spec.-US English	2
9556	6 Slot PCI Riser (Initial order only)	2
9581	RIO-2 Enablement Indicator	2
9911	Power C.-All(Std.Rack P.C.)	2

Product	Description	Quantity
7311-D20	I/O Drawer 1:Model D20 I/O Drawer	2
3147	Remote I/O Cable, 3.5M	4
4651	Rack Indicator, Rack #1	2
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6006	SPCN 3m Cable: Drawer to Drawer	4
6239	2 Gigabit Fibre Channel PCI-X Adapter	4
6268	Power Supply, 435 Watt AC, Hot-swap, Base and Redundant	4
6417	RIO-2 Ports to I/O Planar Riser Card	2
9172	Power Specify, AC	2
9300	Lang Grp Spec.-US English	2
9911	Pwr Cord Spec.- All	2

Product	Description	Quantity
7014-T00	7014-T00 : Rack 1:IBM RS/6000 Rack Model T00	1
6068	Front door (Black) for 1.8M(High Perforation) racks	1
6098	Side panel (black) for 1.8M or 2M racks	2
7176	Power Distribution Unit - Side Mount, Single Phase, L6-30 Connector	1
9176	Pwr Dist Unit Spec.1 Ph.L6-30	1
9300	Language Group US English	1
9800	Power Cord US/Canada	1

SERVIDOR DE SEGURANÇA LÓGICA TIPO 1

Product	Description	Quantity
PIX-535-UR-BUN	535UR Bundle (Chassis, unrestricted SW, 2 FE ports, VAC)	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-BIT 3DES VPN FEATURE LICENSE FOR PIX FIREWALL	1
SF-PIX-6.3	PIX v6.3 Software for the 515/515E, 520, 525 and 535 Chassis	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-VAC-PLUS	VPN Accelerator Card Plus (VAC+) for PIX Firewall	1
PIX-535UR-SW	Unrestricted feature license for PIX 535 Firewall	1
PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1

RQS nº 03/2005 - CN - CPMI - CORREIOS
Pág. 216
FLS Nº 1059

O Servidor de Segurança Lógica Tipo 1, acima, será ofertado na quantidade referida na pág. 234 desta proposta e [illegible]

O Servidor de Segurança Lógica Tipo 2 abaixo será ofertado na quantidade referida na pág. 234 desta Proposta e a especificação unitária constante da Declaração de Casa de Recurso Autorizada.

Itautec

PIX-535-FO-BUN	535FO Bundle (Chassis, failover SW, 2 FE ports, VAC)	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-BIT 3DES VPN FEATURE LICENSE FOR PIX FIREWALL	1
SF-PIX-6.3	PIX v6.3 Software for the 515/515E, 520, 525 and 535 Chassis	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-VAC-PLUS	VPN Accelerator Card Plus (VAC+) for PIX Firewall	1
PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
PIX-535FO-SW	Failover feature license for PIX 535 Firewall	1

0837

SERVIDOR DE SEGURANÇA LÓGICA TIPO 2

Product	Description	Quantity
PIX-525-UR-BUN	525UR Bundle (Chassis, unrestricted SW, 2 FE ports, VAC)	1

SERVIDOR PARA DETECÇÃO DE INTRUSÃO

Product	Description	Quantity
IDS-4250-TX-K9	4250 Sensor (chassis, s/w, SSH, 10/100/1000BaseT w/ RJ-45)	1
CAB-AC	Power Cord,110V	1
IDS-RAIL-2=	2 post Rail Kits for the IDS 4235/4250 Sensor Platforms	1

GERÊNCIA

Product	Description	Quantity
CSACSE-1111-K9	Cisco Secure ACS 3.2 Solution; includes HW and SW	1
CAB-AC	Power Cord,110V	1
CSACSE-3.2-SW-K9	Config. Option; CSACS 3.2 Software loaded on Cisco 1111	1
CSACS-3.2-WIN-K9	Cisco Secure ACS 3.2 for Windows	1

VMS – IDS e PIX FW

Product	Description	Quantity
CWVMS-2.1-UR-K9	VMS 2.1 WIN/SOL Unrestricted HIDS 3DES SW	1
CWVMS-IDS-2.5	License For IDS Host Sensor Console	1

LAN - SWITCHES

Product	Description	Quantity
CWLMS-2.2-K9	LAN Management 2.2 for WIN/SOL; CM, DFM, RME, RTM, CV	1

WAN - ROUTERS

Product	Description	Quantity
CWRW-1.3-K9	Routed WAN Mgmt 1.3 for WIN/SOL; ACL, IPM, RME, CV	1

RQS nº 03/2005 - CN
CORREIOS
Pág. 217
Fls Nº 1057
Doc.

Itautec

4.2 São Paulo

SWITCH TIPO 1

Product	Description	Quantity
WS-C6513	Cat 6513 Chassis, 13slot, 19RU, No Pow Supply, No Fan Tray	1
WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613	1
WS-CAC-2500W	Catalyst 6000 2500W AC Power Supply	1
WS-CAC-2500W/2	Catalyst 6000 Second 2500W AC Power	1
CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL	2
SC6K-S2CVK9-7.6.1	Catalyst 6000 Sup 2 Flash Image w/CV and SSH, Release 7.6.1	1
WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2	1
S6MSF2ZV-12113E	Catalyst 6000 MSFC2 IOS SERVICE PROVIDER W/VIP	1
WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module 2	1
WS-X6516-GBIC	Catalyst 6500 16-port GigE Mod: Fabric-Enabled (Req. GBICs)	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
WS-X6066-SLB-APC	Catalyst 6000 Content Switching Module	1
SC6K-3.1.3-CSM	CSM 3.1.3 Software Release	1
WS-SVC-NAM-1	Catalyst 6500 Network Analysis Module-1	1
SC-SVC-NAM-3.1	Catalyst 6500 NAM SW Release 3.1	1
WS-SVC-FWM-1-K9	Firewall blade for Catalyst 6500	1
SC-SVC-FWM-1.2-K9	Firewall Module Software 1.1(2) for Catalyst 6500	1
WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	18
MEM-S2-128MB	Catalyst 6000 Sup2 Mem, 128MB DRAM Option	1
MEM-MSFC2-128MB	Catalyst 6000 MSFC-2 Mem, 128MB DRAM Option	1
SF-PIX-PDM-2.1	PIX Device Manager for FW Module for Catalyst 6500	1

SWITCH TIPO 2

Product	Description	Quantity
WS-C2950G-48-EI	Catalyst 2950, 48 10/100 with 2GBIC slots, Enhanced Image	1
CAB-AC	Power Cord,110V	1
WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable	1
CAB-RPS-1614=	1 RPS 675 connector cable 16/14	1
WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	1
WS-C2950T-24	24 10/100 ports w/ 2 10/100/1000BASE-T ports, Enhanced Image	1
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable	1
CAB-RPS-1614=	1 RPS 675 connector cable 16/14	1

SCS nº 09/2005 - CN
CPMI - CORREIOS
Fls. Nº 1205
Doc.

9835

Itautec

SWITCH TIPO 3

Product	Description	Quantity
2109-C36	IBM TotalStorage Cabinet C36	1
6080	Ruggedized Rack Feature	1
9200	Quantity of Plant Installed 2109-M12's	1
9751	Brazilian/Portuguese	1
9823	Single Phase Group 2 Cord	1

Product	Description	Quantity
2109-M12	IBM TotalStorage SAN Switch – 128 Port	1
2310	M12 Shortwave SPF Transceiver	128
3216	16port 2Gb Switch Blade	6
5325	M12 Fiber Cable (multimode)	128
7201	Fabric Manager	1
9201	First M12 Installed in 2109-C36	1

SWITCH TIPO 4

Product	Description	Quantity
KV134A-R2	SERVSWITCH AFFINITY - 4 CONSOLES X 16 CPUïS	1
KV131A-R2	SERVSWITCH AFFINITY W/EXPANSION MODUL	7
KV1305C	SERVSWITCH AFFINITY - PLACA DE EMPILHAMENTO	1
EHN382-0100	CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M	120
EHN383-0100	CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M	7

Monitor, Teclado e Mouse

Product	Description	Quantity
31P7453	Teclado ABNT	4
28L3673	Mouse	4
31P8136	Monitor 17" Preto	4

SWITCH TIPO 5

Product	Description	Quantity
CVPN3060-HA-K9	2 Complete VPN 3060 Redundant Systems	1
CAB-AC	Power Cord,110V	1
CVPN3060-SW-K9	Software for VPN3060 Concentrator	1
CAB-AC	Power Cord,110V	1
CVPN3060-SW-K9	Software for VPN3060 Concentrator	1

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1059
Doc.

9824

Itautec

ROTEADOR TIPO 1

Product	Description	Quantity
CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router	1
PWR-3745-AC	AC Power Supply for the Cisco 3745	1
PWR-3745-AC/2	Redundant AC System Power Suppy for the Cisco 3745	1
CAB-AC	Power Cord,110V	2
S374AK9-12301	Cisco 3745 Ser IOS ENTERPRISE PLUS IPSEC 3DES	1
NM-1FE2W	1 10/100 Ethernet 2 WAN Card Slot Network Module	1
WIC-2T	2-PORT SERIAL WAN INTERFACE CARD	2
NM-1A-E3	1-PORT E3 ATM NETWORK MODULE	2
NM-1GE	1 Port GE Network Module	1
WIC-2T	2-PORT SERIAL WAN INTERFACE CARD	2
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	8
WS-G5483=	1000BASE-T GBIC	1

ROTEADOR TIPO 2

Product	Description	Quantity
CISCO1751-V	10/100 Modular Router w/Voice,32F/64D	1
MEM1700-64U96D	Cisco 1751-V 64MB to 96MB DRAM Factory Upgrade	1
S17C7VK9-12215T	Cisco 1700 IOS IP/ADSL/VOICE PLUS IPSEC 3DES	1
WIC-2T	2-PORT SERIAL WAN INTERFACE CARD	1
VIC-2FXO	Two-port Voice Interface Card - FXO	1
VIC-2FXS	Two-port Voice Interface Card - FXS	1
PVDM-256K-4	4-CHANNEL PACKET VOICE/FAX DSP MODULE	1
CAB-AC	Power Cord,110V	1
CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet	1
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	1
PVDM-256K-4	4-CHANNEL PACKET VOICE/FAX DSP MODULE	1
ROUTER-SDM	Device manager for routers	1
PVDM-256K-4	4-CHANNEL PACKET VOICE/FAX DSP MODULE	1

INTEL TIPO 1 (x440)

Product	Description	Quantity
8687-7RX-LM	x440 Xeon MP 2.0GHz/2MB L3 (4way), 2GB	7
59P5188	SMP Expansion Module	7
59P5173	Xeon MP 2.0GHz/2MB L3 proc. upgr.	28
33L3324	512MB PC133 ECC SDRAM RDIMM	84
06P5756	73.4GB 10K U160 SCSI HS HDD	14
06P5740	4Lx	7
24P0960	FC2-133 Host PCI Adapter	14
31P6301	NetXtreme 1000T Ethernet PCI Adapter	21

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 106
Doc.

9833

Itautec

INTEL TIPO 2 (x360)

Product	Description	Quantity
8686-9RX-LM	x360 Xeon MP 2.0GHz/2MB L3 (2way), 2GB	6
59P6817	Xeon MP 2.0GHz/2MB L3 proc. upgr.	12
33L3283	512MB PC1600 ECC DDR SDRAM RDIMM	24
06P5756	73.4GB 10K U160 SCSI HS HDD	12
06P5740	4Lx	6
24P0960	FC2-133 Host PCI Adapter	12
31P6301	NetXtreme 1000T Ethernet PCI Adapter	12
31P6108	370W HS Redundant PS	6

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	24
02R1988	Xeon 3.06GHz/512KB proc. upgr.	24
33L5038	512MB DDR PC2100 ECC RDIMM	48
32P0727	73.4GB 10K U320 SCSI HS HDD	48
31P6301	NetXtreme 1000T Ethernet PCI Adapter	48
59P4211	5U x 24D Tower-to-Rack Kit III	24

RACK

Product	Description	Quantity
9306-420	NB42SR	1
9306-421	NB42SX	4
32P1736	DPI Universal Rack PDU	16
94G6670	Blank Filler Panel Kit	4
94G7448	IEC 320 C14	54

INTEL ADICIONAIS

INTEL TIPO 2 (x360)

Product	Description	Quantity
8686-9RX-LM	x360 Xeon MP 2.0GHz/2MB L3 (2way), 2GB	1
59P6817	Xeon MP 2.0GHz/2MB L3 proc. upgr.	2
33L3283	512MB PC1600 ECC DDR SDRAM RDIMM	4
06P5756	73.4GB 10K U160 SCSI HS HDD	2
06P5740	4Lx	1
24P0960	FC2-133 Host PCI Adapter	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	2
31P6108	370W HS Redundant PS	1

As funcionalidades dos servidores Intel adicionais constam das declarações de esclarecimentos.

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 4061
Doc

9837

Itautec

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
24P0960	FC2-133 Host PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1062
Doc

9831

Itautec

INTEL TIPO 3 (x235)

Product	Description	Quantity
8671-8AX-LM	x235 Xeon 3,06GHz/512KB, 512MB	1
02R1988	Xeon 3.06GHz/512KB proc. upgr.	1
33L5038	512MB DDR PC2100 ECC RDIMM	2
32P0727	73.4GB 10K U320 SCSI HS HDD	2
31P6301	NetXtreme 1000T Ethernet PCI Adapter	1
59P4211	5U x 24D Tower-to-Rack Kit III	1

RISC TIPO 1

Product	Description	Quantity
7040-681	Rack Server 1:pSeries 690 Model 681 CEC	3
2624	32X (Max) SCSI-2 CD-ROM Drive	3
3155	Diskette Drive Cable	3
3255	Operator Panel Attachment Cable	3
4199	128MB Level 3 Cache (4 x 32MB), 567MHz	6
4484	16GB Memory Card, 567MHz, Inward Facing	12
4618	Drawer Placement Indicator, 18U Position, Primary Rack	3
4651	Rack Indicator, Rack #1	3
5246	8-Way POWER4+ Turbo Processor Option	6
5251	Processor Clock Card, Programmable	3
5257	Processor Bus Pass Through Module	6
6158	20/40GB 4mm Internal Tape Drive	3
6161	Cable Group, Power Controller to CEC and Fans	3
6162	Interface Cable, Service Processor to Power Subsystem	3
6170	Power Converter Assembly, Central Electronics Complex	6
6181	Power Cable Group, CEC to Power Controller	3
6182	Power Cable Group, CEC to Power Controller	3
6183	Power Cable Group, CEC to Power Controller	3
6189	DC Power Converter, CEC, Additional	6
6198	Capacitor Book, Two Processor Modules	3
6418	Support Processor with Remote I/O-2 (RIO-2) Loop Attachment, Two Loops	3
6419	Remote I/O-2 (RIO-2) Loop Adapter, Four Loop	3
6565	Backplane, Central Electronics Complex	3
8121	Attachment Cable, Hardware Management Console to Host, 15-Meter	3
8692	Media Drawer, Operator Panel, Diskette	3
9300	Language Group - US English	3

RQS nº 03/2005 - CN
CORREIOS
Pág. 223
Fls. Nº 1067
Doc.

0830

Itautec

Product	Description	Quantity
7040-61D	I/O Drawer 1:Model 61D I/O Drawer	3
2118	Converter Cable, VHDCI to P, Mini-68 pin to 68 pin, 0.3M	3
2122	SCSI Cable - I/O Drawer to Media Drawer	3
2943	8-Port Async Adapter EIA-232/RS-422 (PCI)	6
3125	Serial to Serial Port Cable for Rack/Rack	6
3156	RIO-2 (Remote I/O-2) Cable, 1.75M	12
3277	36.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly	24
4609	Drawer Placement Indicator, 9U Position, Primary Rack	3
4651	Rack Indicator, Rack #1	3
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	24
6121	I/O Drawer Attachment Cable Group, Drawer Position #4609	3
6172	Power Converter Assembly, I/O Drawer	6
6179	Power Cable, I/O Drawer to Media Drawer	3
6203	PCI Dual Channel Ultra3 SCSI Adapter	3
6239	2 Gigabit Fibre Channel PCI-X Adapter	24
6564	Ultra3 SCSI 4-Pack Hot Swap Back Plane	12
6571	I/O Drawer PCI-X Planar, 10 Slot, 2 Integrated Ultra3 SCSI Ports	6
9300	Language Group - US English	3

Product	Description	Quantity
7040-61D I	I/O Drawer 2:Model 61D I/O Drawer	3
2118	Converter Cable, VHDCI to P, Mini-68 pin to 68 pin, 0.3M	3
2943	8-Port Async Adapter EIA-232/RS-422 (PCI)	6
3125	Serial to Serial Port Cable for Rack/Rack	6
3156	RIO-2 (Remote I/O-2) Cable, 1.75M	12
3277	36.4 GB 15,000 RPM Ultra3 SCSI Disk Drive Assembly	24
4605	Drawer Placement Indicator, 5U Position, Primary Rack	3
4651	Rack Indicator, Rack #1	3
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	24
6122	I/O Drawer Attachment Cable Group, Drawer Position #4605	3
6172	Power Converter Assembly, I/O Drawer	6
6203	PCI Dual Channel Ultra3 SCSI Adapter	3
6239	2 Gigabit Fibre Channel PCI-X Adapter	24
6564	Ultra3 SCSI 4-Pack Hot Swap Back Plane	12
6571	I/O Drawer PCI-X Planar, 10 Slot, 2 Integrated Ultra3 SCSI Ports	6
9300	Language Group - US English	3

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 106
Doc

Itautec

Product	Description	Quantity
7040-61R	7040-61R : Rack 1:Model 61R Rack	3
0190	Rack Content: 7040/681 – 17U	3
0191	Rack Content: 7040/61D – 4U	6
0192	Rack Cont: 7040/681 8692 – 1U	3
0193	Rack Cont: 7040/61R 8690 – 8U	3
4651	Rack Indicator, Rack #1	3
6070	Front Door, Black with Copper Accent, Primary Rack	3
6075	Rear Door, Acoustic, Primary or Secondary Rack	3
6186	Bulk Power Regulator	12
6187	Power Controller, Four Cooling Fans, Three DC Power Converter Connections	6
6188	Power Distribution Assembly	6
8678	Line Cord, 6AWG, 14ft, IEC309 Plug	6
8690	Bulk Power Assembly, Redundant	3
9300	Language Group – US English	3

Product	Description	Quantity
7315-C02	HMC 1:Hardware Management Console	2
0966	pSeries Indicator	2
2943	8-Port Async Adapter EIA-232/RS-422 (PCI)	2
3627	IBM P76/P77 Color Monitor, Stealth Black, Captured Cable	2
4962	10/100 Mbps Ethernet PCI Adapter II	2
5005	Software Preinstall (RS)	2
8121	Attachment Cable, Hardware Management Console to Host, 15-Meter	6
8800	Quiet Touch Keyboard - USB, Stealth Black, US English, #103P	2
8841	Mouse - Stealth Black with Keyboard Attachment Cable	2
9004	Southern Hemisphere Designator for Monitors	2
9300	Lang Grp Spec.-US Eng.	2
9800	Power Cord Specify - US/Canada	2

Notebooks - Console

Product	Description	Quantity
2388-BP2	Notebook IBM ThinkPad G40	1

RQS nº 03/2005 - CN
CORREIOS
Pág. 225
Fls. Nº 1065
Doc

Itautec

UNIDADE DE BACKUP

Product	Description	Quantity
3584-L32	IBM UltraScalable Tape Library	1
1462	Fibre Channel Patch Panel	1
1476	LTO Ultrium 2 Fibre Drive Canister	12
1603	Capacity Expansion	1
1662	3584 Specialist	1
1901	Dual AC Power	1
2710	Remote Support Facility	1
6025	25M LC-LC Fibre Channel Cable	28
9212	Attached to Windows System	1
9600	Attached to RS/6000	1
9660	10/100 Ethernet Support	1

Product	Description	Quantity
3589-004	Ultrium cleaning cartridges	1
4005	5-pack Ultrium cleaning cartridge	3

Product	Description	Quantity
3589-006	200GB Ultrium Tape Cartridges with Labeling Services	1
6020	200GB Ultrium Tape Cartridges w/Label 20-pack	20
8000	Jewel Cases	1
9006	Label background color Lt Blue	1
9022	Color/vibrant background	1
9110	First character of Volser is A	1
9200	Second character of Volser is 0	1
9300	Third character of Volser is 0	1
9400	Fourth character of Volser is 0	1
9500	Fifth character of Volser is 0	1

Disco SSA (432GB) para Ambiente de Alta Disponibilidade ITSM - Backup

Product	Description	Quantity
7133-D40	7133-D40 SERIAL DISK SYSTEM -ADVANCED Drawer Model	1
0550	0550 Havant Mfg. Indicator	1
8022	8022 50/60 HZ AC Power Supplies	1
8031	8031 Raven Black Drawer Cover	1
8399	8399 Additional Dummy Drive	10
8572	8572 Advanced 10K rpm/72.8 GB Disk Module	6
8802	8802 2.5 Meter Advanced SSA Cable	4
9300	9300 Language Groups - US English	1

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1066
Doc

Itautec

ITSM - BACKUP

Dois servidores Risc em alta disponibilidade e Rack

Product	Description	Quantity
7028-6C4	ITSM SPM:pSeries 630 Model 6C4 Rack-mount Server	2
2633	CD-ROM Drive - 48X (Max) IDE	2
2848	POWER GXT135P Graphics Accelerator	2
3158	36.4 GB 10,000 RPM Ultra3 SCSI Disk Drive Assembly	4
3254	RIO Cable Support Brackets	2
4250	Connector Cable, 6-slot PCI Riser to Media Bays.	2
4254	SCSI Connector Cable	2
4452	2048MB (4x512MB) SDRAM DIMM Memory	2
4651	Rack Indicator, Rack #1	2
5127	2-way 1.45 GHz POWER4+ Processor Card	2
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6158	20/40GB 4mm Internal Tape Drive	2
6230	Advanced SerialRAID Plus Adapter	2
6239	2 Gigabit Fibre Channel PCI-X Adapter	4
6273	Power Supply ,645 Watt AC, Hot-Swap, Base and Redundant	4
6557	Redundant Cooling	2
6568	Ultra3 SCSI 4-Pack Hot Swap Back Plane	2
9172	Power Specify, AC	2
9300	Lang.Group Spec.-US English	2
9556	6 Slot PCI Riser (Initial order only)	2
9581	RIO-2 Enablement Indicator	2
9911	Power C.-All(Std.Rack P.C.)	2

Product	Description	Quantity
7311-D20	I/O Drawer 1:Model D20 I/O Drawer	2
3147	Remote I/O Cable, 3.5M	4
4651	Rack Indicator, Rack #1	2
5701	IBM 10/10/1000 Base-TX Ethernet PCI-X Adapter	2
6006	SPCN 3m Cable: Drawer to Drawer	4
6239	2 Gigabit Fibre Channel PCI-X Adapter	2
6268	Power Supply, 435 Watt AC, Hot-swap, Base and Redundant	4
6417	RIO-2 Ports to I/O Planar Riser Card	2
9172	Power Specify, AC	2
9300	Lang Grp Spec.-US English	2
9911	Pwr Cord Spec.- All	2

Product	Description	Quantity
7014-T00	Rack 1:IBM RS/6000 Rack Model T00	1
6068	Front door (Black) for 1.8M(High Perforation) racks	1
6098	Side panel (black) for 1.8M or 2M racks	2
7176	Power Distribution Unit - Side Mount, Single Phase, L6-30 Connector	1
9176	Pwr Dist Unit Spec.1 Ph.L6-30	1
9300	Language Group US English	1
9800	Power Cord US/Canada	1

RQS nº 03/2005 - CN
CORREIOS
Pág. 227
Fls. Nº 100
Doc.

Itautec

a926
2

SERVIDOR DE SEGURANÇA LÓGICA TIPO 1

Product	Description	Quantity
PIX-535-UR-BUN	535UR Bundle (Chassis, unrestricted SW, 2 FE ports, VAC)	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-BIT 3DES VPN FEATURE LICENSE FOR PIX FIREWALL	1
SF-PIX-6.3	PIX v6.3 Software for the 515/515E, 520, 525 and 535 Chassis	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-VAC-PLUS	VPN Accelerator Card Plus (VAC+) for PIX Firewall	1
PIX-535UR-SW	Unrestricted feature license for PIX 535 Firewall	1
PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
PIX-535-FO-BUN	535FO Bundle (Chassis, failover SW, 2 FE ports, VAC)	1
CAB-AC	Power Cord,110V	1
PIX-VPN-3DES	168-BIT 3DES VPN FEATURE LICENSE FOR PIX FIREWALL	1
SF-PIX-6.3	PIX v6.3 Software for the 515/515E, 520, 525 and 535 Chassis	1
PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
PIX-VAC-PLUS	VPN Accelerator Card Plus (VAC+) for PIX Firewall	1
PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
PIX-535FO-SW	Failover feature license for PIX 535 Firewall	1

SERVIDOR DE SEGURANÇA LÓGICA TIPO 2

Product	Description	Quantity
PIX-525-UR-BUN	525UR Bundle (Chassis, unrestricted SW, 2 FE ports, VAC)	1

SERVIDOR PARA DETECÇÃO DE INTRUSÃO

Product	Description	Quantity
IDS-4250-TX-K9	4250 Sensor (chassis, s/w, SSH, 10/100/1000BaseT w/ RJ-45)	1
CAB-AC	Power Cord,110V	1
IDS-RAIL-2=	2 post Rail Kits for the IDS 4235/4250 Sensor Platforms	1

GERÊNCIA

Product	Description	Quantity
CSACSE-1111-K9	Cisco Secure ACS 3.2 Solution; includes HW and SW	1
CAB-AC	Power Cord,110V	1
CSACSE-3.2-SW-K9	Config. Option; CSACS 3.2 Software loaded on Cisco 1111	1
CSACS-3.2-WIN-K9	Cisco Secure ACS 3.2 for Windows	1

VMS – IDS e PIX FW

Product	Description	Quantity
CWVMS-2.1-UR-K9	VMS 2.1 WIN/SOL Unrestricted HIDS 3DES SW	1
CWVMS-IDS-2.5	License For IDS Host Sensor Console	1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 228
Fls. Nº 0005
Doc.

Itautec

LAN – SWITCHES

Product	Description	Quantity
CWLMS-2.2-K9	LAN Management 2.2 for WIN/SOL; CM, DFM, RME, RTM, CV	1

WAN - ROUTERS

Product	Description	Quantity
CWRW-1.3-K9	Routed WAN Mgmt 1.3 for WIN/SOL; ACL, IPM, RME, CV	1

4.3 Software Tivoli Brasília

Descrição	PN	Qtd
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC LIC+SW MAINT 12 MO	D51MFLL	432
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC ANNUAL SW MAINT RNWL	E00I9LL	432
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC ANNUAL SW MAINT RNWL	E00I9LL	432
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC ANNUAL SW MAINT RNWL	E00I9LL	432
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR LIC+SW MAINT 12 MO	D51MULL	240
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR ANNUAL SW MAINT RNWL	E00IDLL	240
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR ANNUAL SW MAINT RNWL	E00IDLL	240
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR ANNUAL SW MAINT RNWL	E00IDLL	240
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR LIC+SW MAINT 12 MO	D510ELL	112
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR ANNUAL SW MAINT RNWL	E008ZLL	112
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR ANNUAL SW MAINT RNWL	E008ZLL	112
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR ANNUAL SW MAINT RNWL	E008ZLL	112
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR LIC+SW MAINT 12 MO	D521YLL	128
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR ANNUAL SW MAINT RNWL	E00MHLL	128

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls-Nº 106
Doc.

IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR ANNUAL SW MAINT RNWL	E00MHLL	128
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR ANNUAL SW MAINT RNWL	E00MHLL	128
IBM TIVOLI STORAGE AREA NETWORK MGR PROC LIC+SW MAINT 12 MO	D51M0LL	356
IBM TIVOLI STORAGE AREA NETWORK MGR PROC ANNUAL SW MAINT RNWL	E00I4LL	356
IBM TIVOLI STORAGE AREA NETWORK MGR PROC ANNUAL SW MAINT RNWL	E00I4LL	356
IBM TIVOLI STORAGE AREA NETWORK MGR PROC ANNUAL SW MAINT RNWL	E00I4LL	356
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR LIC+SW MAINT 12 MO	D5102LL	32
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR ANNUAL SW MAINT RNWL	E008VLL	32
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR ANNUAL SW MAINT RNWL	E008VLL	32
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR ANNUAL SW MAINT RNWL	E008VLL	32
IBM TIVOLI STOR MGR EXTENDED ED V5.2.0 MP MEDIA PK ML	BJ09QML	1
IBM TIVOLI STOR MGR FOR SAN 5.2.0 MP MEDIA PK ML	BJ09NML	1
IBM TIVOLI STOR MGR FOR DBS V5.2.0 MP MEDIA PK ML	BJ09UML	1
IBM TIVOLI STOR MGR SYS BAKUP & RECOVERY V5.6 MP MEDIA PK IE	BJ09TIE	1
IBM TIVOLI STOR AREA NETWRK MGR V1.2.0 (N-AP) MP MEDIA PK ML	BJ0AAML	1
IBM TIVOLI STOR MGR FOR MAIL V5.2.0 MP MEDIA PK ML	BJ09XML	1

4.4 Software Tivoli São Paulo

Descrição	PN	Qtd
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC LIC+SW MAINT 12 MO	D51MFLL	194
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC ANNUAL SW MAINT RNWL	E00I9LL	194
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC ANNUAL SW MAINT RNWL	E00I9LL	194
IBM TIVOLI STORAGE MANAGER EXTENDED ED PROC ANNUAL SW MAINT RNWL	E00I9LL	194
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR LIC+SW MAINT 12 MO	D51MULL	104
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR ANNUAL SW MAINT RNWL	E00IDLL	104
IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR ANNUAL SW MAINT RNWL	E00IDLL	104

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1070
Doc.

Itautec

IBM TIVOLI STORAGE MGR FOR STORAGE AREA NW PR ANNUAL SW MAINT RNWL	E00IDLL	104
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR LIC+SW MAINT 12 MO	D510ELL	64
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR ANNUAL SW MAINT RNWL	E008ZLL	64
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR ANNUAL SW MAINT RNWL	E008ZLL	64
IBM TIVOLI STORAGE MANAGER FOR DBS PROCESSOR ANNUAL SW MAINT RNWL	E008ZLL	64
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR LIC+SW MAINT 12 MO	D521YLL	48
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR ANNUAL SW MAINT RNWL	E00MHLL	48
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR ANNUAL SW MAINT RNWL	E00MHLL	48
IBM TIVOLI STG MGR FOR SYSTEM BAKUP AND RECOVER PR ANNUAL SW MAINT RNWL	E00MHLL	48
IBM TIVOLI STORAGE AREA NETWORK MGR PROC LIC+SW MAINT 12 MO	D51M0LL	128
IBM TIVOLI STORAGE AREA NETWORK MGR PROC ANNUAL SW MAINT RNWL	E00I4LL	128
IBM TIVOLI STORAGE AREA NETWORK MGR PROC ANNUAL SW MAINT RNWL	E00I4LL	128
IBM TIVOLI STORAGE AREA NETWORK MGR PROC ANNUAL SW MAINT RNWL	E00I4LL	128
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR LIC+SW MAINT 12 MO	D5102LL	32
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR ANNUAL SW MAINT RNWL	E008VLL	32
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR ANNUAL SW MAINT RNWL	E008VLL	32
IBM TIVOLI STORAGE MGR FOR MAIL PROCESSOR ANNUAL SW MAINT RNWL	E008VLL	32
IBM TIVOLI STOR MGR EXTENDED ED V5.2.0 MP MEDIA PK ML	BJ09QML	1
IBM TIVOLI STOR MGR FOR SAN 5.2.0 MP MEDIA PK ML	BJ09NML	1
IBM TIVOLI STOR MGR FOR DBS V5.2.0 MP MEDIA PK ML	BJ09UML	1
IBM TIVOLI STOR MGR SYS BAKUP & RECOVERY V5.6 MP MEDIA PK IE	BJ09TIE	1
IBM TIVOLI STOR AREA NETWRK MGR V1.2.0 (N-AP) MP MEDIA PK ML	BJ0AAML	1

4.5 Software Compilador C

Product	Description	Quantity
N/A	C FOR AIX - PASSPORT ADVANTAGE - LICENSE, SW SUBSCRIPTION & SUPPORT	
D5A1DLL	C FOR AIX USER LIC/SW MAINT 1 ANNIV	6

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc

BA05IML	IBM C for AIX Version 6.0 MEDIA PK Multilingual	1

4.6 Software de Terceiros

Product	Description	Quantity
Windows e SQL		
P72-00365 / L30116B	Windows Server Ent português Lic/SA Pack Open	56
P73-00396 / L30161B	Windows Server português Lic/SA Pack Open	63
810-01520 / L18973B	SQL Svr Ent Lic/SA Open / 1 Processor License	56
SysEdge		
D5A1DLL	eHealth enhanced SystemEDGE	211

RQS nº 03/2005 - CN
CORREIOS
Pág. 232
Fls. Nº 1078
Doc.

Itautec

5. Aspectos Financeiros

PREGÃO N.º 050/2003 – CPL/AC

1. Razão Social da Empresa: Itautec Informática S.A. – Grupo Itautec Philco

2. CNPJ Nº: 51.764.058/0001-42

3. Inscrição Estadual: 110.970.918.117

4. Inscrição Municipal: 9.077.515-5

5. Endereço Completo Matriz: Rua Santa Catarina, nº 1 – São Paulo – SP

6.Telefone Brasília: (061) 323-3031 ramal 1126 Fax: (61) 226-1251

E-mail: ítalo@itautec.com.br

7. Validade da Proposta: 60 dias, a contar da data da Sessão do Pregão 050/2003– CPL/AC

8. Prazo de Pagamento: conforme edital

9. Banco: 001 – Banco do Brasil S.A. Agência: 3064-3 Conta Corrente: 7999-5

10. Representante da Empresa: Jorge Ítalo Dimatteu Telles

11. Cargo: Representante de Marketing RG: 636.695 – SSP/DF CPF: 292.880.961-91

Apresentamos nossa Proposta para locação de equipamentos de informática – novos de fábrica – incluindo instalação, configuração, treinamento e operação assistida do pessoal encarregado, assistência técnica, garantia e instalação dos PRODUTOS locados, do objeto do Pregão nº 050/2003, acatando todas as estipulações consignadas no Edital.

Declaração de Qualidade:
A Itautec Informática S.A. - Grupo Itautec Philco declara que atende plenamente a todos os atributos técnicos que constituem a configuração mínima obrigatória exigida para o produto em epígrafe.

Declaração de Conformidade:
A Itautec Informática S.A. - Grupo Itautec Philco declara para todos os fins que conhece e aceita todas as condições previstas no Edital desta licitação, bem como nos seus respectivos anexos. Ainda, havendo quaisquer divergências entre sua Proposta e seus catálogos, folders ou manuais, prevalecerá o constante na sua Proposta.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1078
Doc.

Itautec

5.2 Preço Unitário Mensal da Locação dos Produtos

ASPECTOS FINANCEIROS

O VALOR MENSAL DA LOCAÇÃO para cada produto constante das condições específicas da contratação – ANEXOS 1, 1-A e 1-B do Edital e nossa Proposta – para o período de 48 (quarenta e oito) meses, conforme tabela abaixo:

PREÇO MENSAL DA LOCAÇÃO DOS PRODUTOS

TIPO DE PRODUTO	PREÇO MENSAL DE LOCAÇÃO (R$)	DISTRIBUIÇÃO			TOTAL
		CCD AC (DF)		CCD SPM (SP)	
SERVIDOR INTEL TIPO 01	914.126,35	43	14	7	21
SERVIDOR INTEL TIPO 02	353.316,15	25	29	6	35
SERVIDOR INTEL TIPO 03	316.206,07	12	27	24	51
SERVIDOR RISC TIPO 01	1.074.638,07		8	3	11
SWITCH TIPO 01	187.013,19	12	2	2	4
SWITCH TIPO 02	16.313,07	04	4	2	6
SWITCH TIPO 03	266.485,53	50	4	2	6
SWITCH TIPO 04	109.263,26	24	8	4	12
SWITCH TIPO 05	48.263,97	96	1	1	2
ROTEADOR TIPO 01	25.708,23	22	1	1	2
ROTEADOR TIPO 02	7.854,43	12	2	0	2
UNIDADE DE BACKUP ROBOTIZADO	316.077,46		1	1	2
SERVIDOR DE SEGURANÇA LÓGICA TIPO 01	373.274,60		2	2	4
SERVIDOR DE SEGURANÇA LÓGICA TIPO 02	27.579,76		1	1	2
SERVIDOR PARA DETECÇÃO DE INTRUSÃO	22.106,71	70	1	1	2
TOTAL MENSAL DE LOCAÇÃO	4.058.226,78	89	105	57	162

Nestes valores estão inclusos: a instalação dos PRODUTOS, a assistência técnica, o treinamento, as despesas decorrentes dos deslocamentos de técnicos para atendimento dos chamados, frete, seguros (contra incêndio, roubo, danos elétricos ou provenientes de fenômenos da natureza), impostos/taxas e demais despesas com peças e acessórios, bem como todas as despesas decorrentes do cumprimento integral do objeto do Edital.

O VALOR TOTAL DA LOCAÇÃO é o resultado do VALOR MENSAL DA LOCAÇÃO multiplicado por 48 (quarenta e oito), que representa o número de meses de locação.

RQS nº 03/2005 - CORREIOS
CPMI
Fls. Nº
Doc.

Itautec

Apresentação do Cronograma de Trabalho, conforme ANEXO 1-A, item 1.2. do Edital, fica estipulado em 1% (um por cento) do VALOR TOTAL DA LOCAÇÃO, subitem 1.2 desta Proposta, para fins do primeiro pagamento .

O VALOR GLOBAL DA PROPOSTA é o resultado do somatório dos itens: VALOR TOTAL DA LOCAÇÃO (1.2.) e do Cronograma de Trabalho (1.3.)

5.3 Discriminação dos Valores

VALOR TOTAL DA LOCAÇÃO (somatório dos 48 meses de aluguel)	~~R$194.794.885,44~~ 194.794.890,70
APRESENTAÇÃO DO CRONOGRAMA DE TRABALHO (1% do Valor Total da Locação)	R$ 1.947.948,~~85~~ 90
VALOR GLOBAL DA PROPOSTA (VALOR TOTAL DA LOCAÇÃO + Cronograma de Trabalho)	~~R$196.742.834,29~~ 196.742.839,60

RQS nº 03/2005 - CN
CPMI - CORREIOS
Pág. 235
Fls. Nº 1075
Doc.

Itautec

5.4 Planilha detalhada de custo de formação do preço mensal da locação

A Itautec apresenta planilha detalhada de custo de formação do preço mensal da locação, em atendimento a exigência constante no subitem 5.8. do edital conforme abaixo:

ITEM (especificar percentual de cada um)	PERCENTUAL
1. EQUIPAMENTOS:	
Subtotal	33,099%
2. SOFTWARE:	
Subtotal	4,121%
3. TREINAMENTOS	
Subtotal	40,830%
4. ASSISTÊNCIA TÉCNICA / GARANTIA	
Subtotal	7 %
5. INSTALAÇÃO	
Subtotal	0,616%
6. TRIBUTOS	
Subtotal	10,8%
7. TRANSPORTE / FRETE / SEGURO	
Subtotal	0,389%
8. DESPESAS ADMINISTRATIVAS	
Subtotal	1,640%
9. OUTROS CUSTOS E MARGEM	
Subtotal	1,506%
TOTAL	100%

Declarações que acompanham esta Proposta Econômica

- A Itautec declara de que irá dispor de central de atendimento telefônico com discagem gratuita e/ou via internet, para processo de recepção, qualificação, controle e solução dos chamados de manutenção corretiva, conforme segue no Anexo 2;

- Declaração dos fabricantes e/ou distribuidores autorizados, nos casos em que o proponente não seja o fabricante dos equipamentos, em papel timbrado e com firma (s) reconhecida (s), mencionando o número e o objeto deste Edital, assegurando que os equipamentos cotados são de linha de produção continuada, que segue em anexo.

ROS nº 031/2005 - CN
CPMI - CORREIOS
Fls. Nº 1070
Doc.

Itautec

- Carta de solidariedade emitida pelo fabricante, em papel timbrado e com firma reconhecida, nos casos em que o proponente não seja o fabricante dos equipamentos, ofertados nesta Proposta Econômica (Servidores, Switches, Roteadores e Unidade de Backup Robotizado), mencionando o número e o objeto deste edital, que segue em anexo.

- Declaração de responsabilidade nos componentes de terceiros, utilizados na solução da proponente, que segue em anexo.

- Certificado PMP (Project Management Professional) emitido em favor do gestor do projeto alocado pelo PMI (Project Management Institute), que segue em anexo.

- Atestados de Vistoria, emitidos pela ECT, conforme MODELO VI constante do ANEXO 3 do Edital, nas instalações dos Centros Corporativos de Dados localizados em Brasília-DF e São Paulo-SP, que seguem em anexo.

- Garantia do objeto: A Itautec garante o objeto dessa licitação pelo prazo de 48 (quarenta e oito) meses (periodo de locação), conforme exigido no Edital.

- A Itautec declara disponibilizar os PRODUTOS no prazo de 60 (sessenta) dias após o término da vigência do Contrato, conforme descrito no subitem 2.18. da cláusula segunda do ANEXO 2 do Edital.

A Itautec, reitera que tomou conhecimento de todas as informações e condições para o cumprimento das obrigações objeto desta licitação e que atende todas as condições do Edital.

Brasília – DF, 24 de julho de 2003.

Itautec Informática S.A
Grupo Itautec Philco
Jorge Ítalo Dimatteu Telles
Representante de Marketing

Itautec Informática S.A.
Grupo Itautec Philco
Raimundo Carlos Pereira
Gerente Comercial

RQS nº 03/2005 - CN
CORREIOS
Pág. 237
Fls. Nº 107
Doc.

Itautec

9816
-21

ANEXO 01 – ATESTADOS DE VISTORIA

RDS nº 03/2005 - CN
ADMI - CORREIOS
Fls. Nº 1078
Doc.

CORREIOS **ADMINISTRAÇÃO CENTRAL**

ATESTADO DE VISTORIA

Atestamos para fins de Licitação, relativamente ao Edital do Pregão n.º 050/2003- CPL/AC, cujo objeto é a locação de equipamentos de informática, que o Sr(a) LUIS GUSTAVO G. DE MELO, representante da empresa ITAUTEC PHILCO S/A, esteve visitando nesta data, as instalações físicas do Centro Corporativo de Dados de BRASILIA, visando obter subsídios para a proposta econômica da licitação em questão.

1. Responsável pelo Termo de Vistoria
   Nome em letra de forma: ROBERTO STEFAN F. DE AGUIAR
   Matrícula: 8011879-8
   Assinatura: _____
   Data: 21/07/2003.

2. Representante da Licitante
   Nome em letra de forma: LUIS GUSTAVO G. DE MELO
   Assinatura: _____
   Data: 21/07/2003.

Brasília-DF, 21 de Julho de 2003.

OBSERVAÇÕES:

- Os interessados em participar desta Licitação deverão realizar, ***obrigatoriamente***, vistoria nos Centros Corporativos de Dados de Brasília e São Paulo, devidamente acompanhada de representante da ECT.
  Os endereços dos CCDs são os seguintes:
  Brasília : SBN - QUADRA 01- BLOCO A - 2º SUBSOLO - ED. SEDE ECT - BRASÍLIA/DF
  São Paulo : RUA MERGENTHALER, N° 592 – BLOCO 3 – 4° ANDAR – VILA LEOPOLDINA CEP: 05311-900 SÃO PAULO – SP
- As vistorias deverão ocorrer no prazo de até **02 (dois) dias úteis** antes da data de abertura da licitação, objetivando conhecer, principalmente, as características técnicas do ambiente e os locais de instalação dos produtos.
- O agendamento das vistorias deverá ser previamente efetuado junto aos seguintes telefones:
  Brasília: (0xx61) 426-2214/1754/1896
  São Paulo: (0xx11) 3838-7755/7000/7001

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 1079 Doc

CORREIOS ADMINISTRAÇÃO CENTRAL

ANEXO 3

(MODELO VI)

ATESTADO DE VISTORIA

Atestamos para fins de Licitação, relativamente ao Edital do Pregão n.º 050/2003- CPL/AC, cujo objeto é a locação de equipamentos de informática, que o Sr(a) Ricardo Riiuti Kameoka, representante da empresa Etantec Informatica S.A., esteve visitando nesta data, as instalações físicas do Centro Corporativo de Dados de São Paulo SPM, visando obter subsídios para a proposta econômica da licitação em questão.

1. Responsável pelo Termo de Vistoria
   Nome em letra de forma: Olavo de Brito
   Matrícula: 8.918438-6
   Assinatura: _____
   Data: 21/07/2003.

2. Representante da Licitante
   Nome em letra de forma: Ricardo Riiuiti Kameoka
   Assinatura: _____
   Data: 21/07/2003.

São Paulo
~~Brasília~~-DF, 21 de julho de 2003.

OBSERVAÇÕES:

- Os interessados em participar desta Licitação deverão realizar, ***obrigatoriamente***, vistoria nos Centros Corporativos de Dados de Brasília e São Paulo, devidamente acompanhada de representante da ECT.
  Os endereços dos CCDs são os seguintes:
  Brasília : SBN - QUADRA 01- BLOCO A - 2º SUBSOLO - ED. SEDE ECT - BRASÍLIA/DF
  São Paulo : RUA MERGENTHALER, N° 592 – BLOCO 3 – 4° ANDAR – VILA LEOPOLDINA CEP: 05311-900 SÃO PAULO – SP
- As vistorias deverão ocorrer no prazo de até **02 (dois) dias úteis** antes da data de abertura da licitação, objetivando conhecer, principalmente, as características técnicas do ambiente e os locais de instalação dos produtos.
- O agendamento das vistorias deverá ser previamente efetuado junto aos seguintes telefones:
  Brasília: (0xx61) 426-2214/1754/1896
  São Paulo: (0xx11) 3838-7755/7000/7001

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1054
Doc.

Itautec

ANEXO 2 – DECLARAÇÕES E CERTIFICAÇÕES

SCS Q. 01 Bloco "F" 11º Andar – Ed. Camargo Corrêa – Brasília-DF CEP: 70397-900 - Fone: (61) 323-3031 Fax: (61) 226-1251

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 1081
Doc.

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante dos Servidores RISC p690 e p630, em referência ao Edital do Pregão n.º 083/2002-CPL/AC declara que:

- As fontes internas do servidor IBM eServer pSeries p690 estão instaladas na configuração máxima do equipamento, conforme item 4.2.1 SERVIDORES RISC TIPO 1 do Anexo 02.
- Os equipamentos serão novos de fábrica e serão entregues acondicionados adequadamente em caixas fechadas, de forma a permitir completa segurança durante o transporte, conforme item 2.3 REQUISITOS GERAIS do Anexo 1B;
- Serão fornecidos, quando da entrega e instalação dos produtos, todos os cabos, acessórios, manuais e documentações completas, que são necessários ao pleno funcionamento dos equipamentos, softwares e periféricos, conforme item 2.3 REQUISITOS GERAIS do Anexo 1B;
- Os equipamentos p690 propostos como RISC Tipo 01 estão sendo ofertados com, no mínimo 8 (oito) partições físicas e ou lógicas e são expansíveis a 32 partições físicas e ou lógicas, conforme item 2.7 REQUISITOS GERAIS do Anexo 1B;
- O número especificado de partições é alcançado com a simples configuração de software fornecido para este fim, sem a necessidade de adição de nenhum hardware ou software adicionais, conforme item 2.7 REQUISITOS GERAIS do Anexo 1B;
- Estão sendo ofertadas 2 (duas) consoles em cada localidade, sendo que todas as consoles gerenciam todos os equipamentos em cada localidade, conforme item 2.7 REQUISITOS GERAIS do Anexo 1B;
- As partições funcionam de modo que cada uma executa sua própria imagem de sistema operacional e que a falha do sistema operacional de uma partição não interfere, em hipótese alguma, no funcionamento das demais partições, conforme item 2.7 REQUISITOS GERAIS do Anexo 1B;
- As fontes de alimentação propostas para os servidores RISC Adicionais são redundantes por fontes internas independentes, com alimentação redundante, de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2(dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações, conforme item 2.10 RECURSOS MÍNIMOS DE HARDWARE E SOFTWARE PARA OS SERVIDORES RISC ADICIONAIS do Anexo 1B;
- As interfaces de rede irão conectar os servidores RISC adicionais a Rede do CCD são capazes de utilizar cabeamento UTP CAT-6 e conectores RJ45, conforme item

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1082
Doc.

IBM BRASIL - INDÚSTRIA, MÁQUINAS E SERVIÇOS LTDA.
SCN Q. 4 Bl. B - 7º andar Centro Empresarial Varig
Brasília- DF Cep: 70.710-500
Telefone: (61) 329-2800 Fax: (61) 329 2850
C.N.P.J.: 33.372.251/0100-38 Insc. Es.: 07.333.522/002-44

Carta de Solidariedade

À EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS – ECT
SBN – Quadra 01, Bloco "A" – Sobreloja – Ed. Sede ECT
Fax: (61) 426-2759

Ref: Edital do Pregão ECT nº 050/2003 – Objeto: locação e instalação de 162 (cento e sessenta e dois) equipamentos de informática – novos de fábrica - incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo.

Vimos, por meio desta, apresentar nossa solidariedade com a Itautec Informática S.A. - Grupo Itautec Philco, CNPJ 51.764.058/0001-42, Rua Santa Catarina, 1 - São Paulo - SP, no Edital supracitado, que estamos solidários a esta, garantindo o fornecimento dos seguintes produtos:

TIPO DE PRODUTO	MARCA	MODELO
SERVIDOR INTEL TIPO 01	IBM	xSeries 440
SERVIDOR INTEL TIPO 02	IBM	xSeries 360
SERVIDOR INTEL TIPO 03	IBM	xSeries 235
SERVIDOR RISC TIPO 01	IBM	pSeries 690
SWITCH TIPO 01	Cisco	Catalyst 6513
SWITCH TIPO 02	Cisco	Catalyst 2950
SWITCH TIPO 03	IBM	2109-M12
SWITCH TIPO 04	Black Box	Afinity
SWITCH TIPO 05	Cisco	CVPN 3060
ROTEADOR TIPO 01	Cisco	Cisco 3745
ROTEADOR TIPO 02	Cisco	Cisco 1751-V
UNIDADE DE BACKUP ROBOTIZADO	IBM	LTO Ultrium 3584
SERV. DE SEGURANÇA LÓGICA TIPO1	Cisco	PIX - 535
SERV. DE SEGURANÇA LÓGICA TIPO2	Cisco	PIX - 525
SERV. P/ DETECÇÃO DE INTRUSÃO	Cisco	IDS - 4250
SERVIDOR RISC ADICIONAL	IBM	PSeries 630
Notebooks	IBM	Notebook IBM ThinkPad G40

Adicionalmente atestamos:

a) nossa solidariedade com a Itautec no âmbito dos produtos acima listados, quanto aos compromissos por ela assumidos na licitação supra-citada;
b) Que a Itautec está apta a prestar assistência técnica, com o uso de peças e

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. 1018
Doc.

IBM

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que "as licenças de software que desempenha as funções de um **GERENCIADOR DE FITOTECA E DE BACKUP** serão fornecidas considerando-se o número de unidades de backup solicitadas e o número total de servidores fornecidos", conforme item 5 - Unidade de Backup subitem 13 – Recursos de Software do Anexo 01-B do Edital do Pregão n.º 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

15o CARTORIO DE NOTAS DE SAO PAULO
Rua da Gloria, 98 - Fone:(0XX11) 3105-9194/98
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
Reco por SEMELHANCA 0001 FIRMA(S) DE:
CARMEM LUCIA TAVORA VIEIRA
SAO PAULO, 23 de JULHO de 2003.
SERVENTE:MIGUEL PERES JUNIOR
60:ESCREVENTE AUTORIZADO.....
S.:R$2,07 Digitado Por
Sob:220593
PAGOS POR VERBA

Colegio Notarial do Brasil
FIRMA
1059AA009400

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1084
Doc.

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.° 33.372.251/0001-56, na condição de fabricante, declara que a interface de vídeo dos servidores IBM eServer xSeries 440 e xSeries 360 são PCI 32bits, conforme item 4.1.1 SERVIDORES INTEL TIPO 1, sub-item 6 e item 4.1.2 SERVIDORES INTEL TIPO 2, sub-item 6 do Anexo 02 do Edital do Pregão n.° 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

5o CARTORIO DE NOTAS DE SÃO PAULO
Rua da Gloria, 98 - Fone:(0XX11) 3105-9194/98
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
reco por SEMELHANCA 0001 FIRMA(S) DE:
ARMEM LUCIA TAVORA VIEIRA
AULO, 23 de JULHO de 2003
IMANTE:MIGUEL PERES JUNIOR
GO:ESCREVENTE AUTORIZADO
s.:******2,07
bo:220596
PAGOS POR VERBA
Validado Por

Colegio Notarial do Brasil
FIRMA 1
1059AA009403

RGS 07/03/2003 - CN
CPMI - CORREIOS
Fls Nº 1085

Doc.

IBM

4806

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que " serão fornecidos 2 (dois) equipamentos servidores RISC Para o CCD de Brasília, em alta disponibilidade, para abrigar os softwares gerenciadores das fitotecas e os softwares gerenciadores do backup e também será fornecido 2 (dois) servidores RISC para o CCD de São Paulo, em alta disponibilidade, para abrigar o software gerenciador da fitoteca e o software gerenciador do backup; Os servidores estão dimensionados de tal forma que suportem o gerenciamento de 150 clientes de backup, individualmente.", conforme item 5 - Unidade de Backup subitem 15 - Geral do Anexo 01-b do Edital do Pregão n.º 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

15o CARTORIO DE NOTAS DE SAO PAULO
Rua da Gloria, 98 - Fone:(0XX11) 3105-
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
Reconheco por SEMELHANCA 0001 FIRMA(S) DE:
0001-CARMEM LUCIA TAVORA VIEIRA
SAO PAULO, 23 de JULHO de 2003
ASSINANTE:MIGUEL PERES JUNIOR
CARGO:ESCREVENTE AUTORIZADO
Custas.:
Carimbo:220596
SELOS PAGOS POR VERBA
FIRMA 1
1059AA009405

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1086
Doc.

IBM

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que " há compatibilidade e integração com as versões dos equipamentos existentes: Switches: Modelo 2109 - S16 fabricante IBM (OEM Brocade 2800 Silkworm), versão de microcódigo A2.4.1C; Storage Modelo 2105 - F20 (IBM) com dois microcódigos (2 dispositivos de armazenamento) 1.5.2.103 e 1.3.2.49; HBA`s Modelo Qlogic QLA 2200 - PCI Fibre Channel adpater, versão de microcódigo 8.0.8.1" , conforme item 3.3 SWITCH TIPO 3 (FC) subitem 5 - Compatibilidade e Integração do Anexo 01-b do Edital do Pregão n.º 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

15º Tab. Cam...

15o CARTORIO DE NOTAS DE SAO PAULO
Rua da Gloria, 98 - Fone:(0XX11) 3105-
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
Confiro por SEMELHANCA 0001 FIRMA(S) DE:
CARMEN LUCIA TAVORA VIEIRA
SAO PAULO, 23 de JULHO de 2003.
SINANTE:MIGUEL PERES JUNIOR
ARGO:ESCREVENTE AUTORIZADO.....
is.:*******2,07
mbo:220597
S PAGOS POR VERBA

Colegio Notarial do Brasil SP
FIRMA 1
1059AA009404

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1087
Doc.

CISCO SYSTEMS

São Paulo, 21 de julho de 2003

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

Re.: **PREGÃO N.º 050/2003 - CPL/AC**

Prezados Senhores,

Versão em inglês para referência apenas
English version for reference only

Declaramos para fins do pregão acima que **ITAUTEC INFORMÁTICA S.A. - GRUPO ITAUTEC PHILCO**, inscrita no CNPJ/MF sob o nº 51.764.058/0001-42, com sede na Rua Santa Catarina, 01 - Parte Prédio 18 - Tatuapé - São Paulo - SP, doravante EMPRESA, é revendedor autorizado Cisco no Brasil.

We hereby inform for the purposes of the above process that **ITAUTEC INFORMÁTICA S.A. - GRUPO ITAUTEC PHILCO**, inscrita no CNPJ/MF sob o nº 51.764.058/0001-42, com sede na Rua Santa Catarina, 01 - Parte Prédio 18 - Tatuapé - São Paulo - SP, hereinafter COMPANY is an authorized reseller in Brazil.

Asseguramos para fins do certame em referência:

We certify for the purposes of the above process:

- o fornecimento e a garantia dos produtos Cisco no anexo relacionados; e que
- os equipamentos Cisco cotados pela EMPRESA, relacionados no anexo são de linha de produção continuada e que serão fornecidas peças de reposição pelo período mínimo de 60 (sessenta) meses.

- the supply and warranty of the Cisco products listed in the attachment hereto; and that
- the Cisco equipment offered by COMPANY are from a continued line of production and that spare parts will be available for a minimum period of 60 (sixty) months.

Atestamos ainda, com relação aos equipamentos Cisco relacionados no anexo:

We also certify with regards to the Cisco products listed in the attachment hereto:

a) nossa solidariedade para com a EMPRESA no âmbito dos produtos Cisco quanto aos compromissos que a EMPRESA venha a assumir perante a ECT, no escopo desta licitação;

a) our joint liability with COMPANY with regards to Cisco products in relation to the obligations that COMPANY commits before ECT, within this process;

b) que a EMPRESA está apta a prestar assistência técnica, com o uso de peças e componentes originais, bem como suporte aos produtos Cisco cotados;

b) that COMPANY is capable of rendering technical assistance, with the use of original spare parts, as well as support to the Cisco products offered;

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1088
Doc.

CISCO SYSTEMS

c) nossa responsabilidade solidária para com a EMPRESA pelo perfeito cumprimento das exigências de garantia dos produtos Cisco, durante todo o prazo de vigência do contrato.

c) our joint liability responsibility with COMPANY for the perfect fulfillment of warranty of Cisco products, during the whole term of the agreement.

Atenciosamente,

Cisco do Brasil Ltda
Sérgio Tsujioka
Representante Legal

CONFERIDO POR

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE:
001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 22 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
ALCIDES BATISTA CORREIA-ESC. AUTORIZ.
Total Custas.:*****2,07
Cod.:1337030 DOC.S/V.ECONOMICO
Selo:1063AA055808

Colégio Notarial do Brasil - SP
FIRMA 1
1063AA055808
Marcio Roberto Trofino
Escrevente Autorizado

.o Trofino
utorizado

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1082
Doc.

EQUIPAMENTOS DE REDE EDITAL Correios 050_2003

Itautec

SWITCH TIPO 1

Cód.	Product	Description	Quant
	WS-C6513	Cat 6513 Chassis, 13slot, 19RU, No Pow Supply, No Fan Tray	1
	WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613	1
	WS-CAC-2500W	Catalyst 6000 2500W AC Power Supply	1
	WS-CAC-2500W/2	Catalyst 6000 Second 2500W AC Power	1
	CAB-AC-2500W-INT	Power Cord, 250Vac 16A, INTL	2
	S6S22ZK2-12119E	Catalyst 6000 SUP2/MSFC2 IOS SP W/VIP SSH 3DES	1
	WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2	1
	WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module 2	1
	WS-X6516A-GBIC	Catalyst 6500 16-port GigE Mod, fabric-enabled (Req. GBICs)	1
	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
	MEM-DFC-128MB	128 MB DRAM FOR DFC	1
	WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
	WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
	WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	1
	WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
	MEM-DFC-128MB	128 MB DRAM FOR DFC	1
	WS-X6066-SLB-APC	Catalyst 6000 Content Switching Module	1
	SC6K-3.1.3-CSM	CSM 3.1.3 Software Release	1
	WS-SVC-NAM-1	Catalyst 6500 Network Analysis Module-1	1
	SC-SVC-NAM-3.1	Catalyst 6500 NAM SW Release 3.1	1
	WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
	MEM-DFC-128MB	128 MB DRAM FOR DFC	1
	WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
	MEM-DFC-128MB	128 MB DRAM FOR DFC	1
	WS-X6516-GE-TX	Catalyst 6500 16-port Gig/Copper Module, x-bar	1
	WS-F6K-DFC	Dist Fwd Card for 65xx, 6816 Modules used with SUP1A/SUP2	1
	MEM-DFC-128MB	128 MB DRAM FOR DFC	1
	WS-G5484	1000BASE-SX Short Wavelength GBIC (Multimode only)	16
	MEM-S2-128MB	Catalyst 6000 Sup2 Mem, 128MB DRAM Option	1
	MEM-MSFC2-128MB	Catalyst 6000 MSFC-2 Mem, 128MB DRAM Option	1

SWITCH TIPO 2

Cód.	Product	Description	Quant
	WS-C2950G-48-EI	Catalyst 2950, 48 10/100 with 2 GBIC slots, Enhanced Image	1
	CAB-AC	Power Cord,110V	1
	WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)	1
	WS-X3500-XL	GigaStack Stacking GBIC and 50cm cable	1
	PWR300-AC-RPS-N1	Redundant Power System 300 (RPS 300) w/ 1 connector cable	1
	CAB-AC	Power Cord,110V	1

SWITCH TIPO 5 (CONCENTRADOR DE VPNs)

Cód.	Product	Description	Quant
	CVPN3060-NR	VPN 3060 Concentrator (Non-Redun, 1 P/S); 5000users@100Mbps	1
	CVPN3060-SW-K9	Software for VPN3060 Concentrator	1

RGS Nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 107
Doc

	CAB-AC	Power Cord,110V	1
	CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply	1

SERVIDOR DE AUTENTICAÇÃO PARA O SWITCH TIPO 5

Cód.	Product	Description	Quant
	CSACSE-1111-K9	Cisco Secure ACS 3.2 Solution; includes HW and SW	1
	CAB-AC	Power Cord,110V	1
	CSACSE-3.2-SW-K9	Config. Option; CSACS 3.2 Software loaded on Cisco 1111	1

ROTEADOR TIPO 1

Cód.	Product	Description	Quant
	CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router	1
	PWR-3745-AC	AC Power Supply for the Cisco 3745	1
	PWR-3745-AC/2	Redundant AC System Power Suppy for the Cisco 3745	1
	CAB-AC	Power Cord,110V	2
	S374AK9-12301	Cisco 3745 Ser IOS ENTERPRISE PLUS IPSEC 3DES	1
	NM-1FE2W	1 10/100 Ethernet 2 WAN Card Slot Network Module	1
	WIC-2T	2-Port Serial WAN Interface Card	2
	NM-1A-E3	1-Port E3 ATM Network Module	2
	NM-1GE	1 Port GE Network Module	1
	WIC-2T	2-Port Serial WAN Interface Card	2
	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	8
	WS-G5483=	1000BASE-T GBIC	1

ROTEADOR TIPO 2

Cód.	Product	Description	Quant
	CISCO1751-V	10/100 Modular Router w/Voice,32F/64D	1
	MEM1700-64U96D	Cisco 1751-V 64MB to 96MB DRAM Factory Upgrade	1
	S17C7HVK9-12208T	Cisco 1700 IOS IP/ADSL/VOICE/FW/IDS PLUS IPSEC 3DES	1
	WIC-2T	2-Port Serial WAN Interface Card	1
	VIC-2FXO	Two-port Voice Interface Card - FXO	1
	VIC-2FXS	Two-port Voice Interface Card - FXS	1
	PVDM-256K-4	4-Channel Packet Voice/Fax DSP Module	1
	CAB-AC	Power Cord,110V	1
	CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet	1
	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	1
	PVDM-256K-4	4-Channel Packet Voice/Fax DSP Module	1

SERVIDOR DE SEGURANÇA LÓGICA TIPO 1

Cód.	Product	Description	Quant
	PIX-535	PIX Firewall 535 Chassis	1
	CAB-AC	Power Cord,110V	1
	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
	PIX-535UR-SW	Unrestricted feature license for PIX 535 Firewall	1
	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1091
Doc.

	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
	PIX-535-PWR-AC	Redundant AC power supply for PIX 535	1
	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
	PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
	PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535	1
	PIX-535	PIX Firewall 535 Chassis	1
	CAB-AC	Power Cord,110V	1
	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
	PIX-535FO-SW	Failover feature license for PIX 535 Firewall	1
	SF-PIX-6 2	PIX v6 2 Software for the PIX 515E, 525 and 535 Chassis	1
	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
	PIX-535-PWR-AC	Redundant AC power supply for PIX 535	1
	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
	PIX-1FE	Single 10/100 Fast Ethernet Inteface for PIX Firewall, RJ45	1
	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
	PIX-535-MEM-512	PIX 535 512MB RAM Upgrade (2-256MB DIMM, UR Only)	1
	PIX-535-PWR-BLANK	Blank to fill unused power supply slot on PIX 535	1

SERVIDOR DE SEGURANÇA LÓGICA TIPO 02

Cód.	Product	Description	Quant
	PIX-525	PIX Firewall 525 Chassis	1
	CAB-AC	Power Cord,110V	1
	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
	PIX-525-SW-UR	Unrestricted feature license for PIX 525 Firewall	1
	SF-PIX-6 2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1
	PIX-525	PIX Firewall 525 Chassis	1
	CAB-AC	Power Cord,110V	1
	PIX-VPN-3DES	168-bit 3DES VPN feature license for PIX Firewall	1
	PIX-525-SW-FO	Failover feature license for PIX 525 Firewall	1
	SF-PIX-6.2	PIX v6.2 Software for the PIX 515E, 525 and 535 Chassis	1
	PIX-4FE-66	PIX 66-MHz Four-port 10/100 Ethernet Interface, RJ45	1
	PIX-1GE-66	66MHz Gigabit Ethernet Interface, Multimode (SX) SC	1
	PIX-VPN-ACCEL	VPN Accelerator Card for PIX 515E/525/535-UR/FO Firewall	1

SISTEMA PARA DETECÇÃO DE INTRUSÃO

Cód.	Product	Description	Quant
	IDS-4250-TX-K9	4250 Sensor (chassis, s/w, SSH, 10/100/1000BaseT w/ RJ-45)	1
	CAB-AC	Power Cord,110V	1

SOFTWARE DE GERENCIAMENTO DE SEGURANÇA E VPN

Cód.	Product	Description	Quant
	CWVMS-2 2-UR-K9	VMS 2.2 WIN/SOL Unrestricted	1
	CWVMS-MCCSA-4 0	Expanded Part use Only: MC for Cisco Security Agents 4.0	1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1063
Doc.

SOFTWARE DE GERENCIAMENTO DE LAN

Cód.	Product	Description	Quant
	CWLMS-2.2-K9	LAN Managment 2.2 for WIN/SOL; CM, DFM, RME, RTM, CV	1

SOFTWARE DE GERENCIAMENTO DE WAN

Cód.	Product	Description	Quant
	CWRW-1.3-K9	Routed WAN Mgmt 1.3 for WIN/SOL; ACL, IPM, RME, CV	1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1093
Doc.

Cisco do Brasil Ltda.
Av. Nações Unidas, 12.901 - 26° and.
04578-000 - São Paulo – SP
Tel.: (011) 5508-9999
Fax: (011) 5508-9998
www.cisco.com

São Paulo, 21 de julho de 2003

A
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

Ref.: **PREGÃO N.º 050/2003 - CPL/AC**

Prezados Senhores,

Declaramos, para fins de comprovação no edital em epígrafe que a empresa **MULTIREDE INFORMÁTICA LTDA.**, inscrita no CNPJ/MF sob o número 66.060.088/0001-45 e localizada na rua Dr. Eduardo de Souza Aranha, 387 – Itaim Bibi – São Paulo - SP é atualmente parceiro certificado pela Cisco Systems, Inc. como **Cisco Learning Solutions Partner**.

Esclarecemos por oportuno que os cursos CWFUN e CWLAW foram descontinuados e substituídos pelo curso CWENT.

CONFERIDO POR

Atenciosamente,

Cisco do Brasil Ltda.
Sergio Tsujioka
Representante Legal

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE:
001-SERGIO FUMIAKI TSUJIOKA
SAO PAULO, 22 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
MARCIO ROBERTO TROFINO-ESC. AUTORIZ.
Total Custas.:*****2,07
Car.:1336969 DOC.S/V.ECONOMICO
Selo:1063AA055784

Colegio Notarial do Brasil SP
FIRMA
1063AA055784
Marcio Roberto Trofino
Escrevente Autorizado

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1091
Doc.

CISCO SYSTEMS

São Paulo, 22 de julho de 2003

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT

Re.: **PREGÃO N.º 050/2003 - CPL/AC**

Prezados Senhores,

Informamos abaixo algumas características técnicas dos produtos Cisco abaixo relacionados:

1) As fontes de alimentação do concentrador Cisco VPN 3060 possuem recurso de troca sem interrupção (HOT-SWAPPABLE/HOT-PLUGGABLE).

2) O roteador Cisco 3745 possui capacidade de roteamento de até 225.000 (duzentos e vinte e cinco mil) pacotes por segundo, utilizando pacotes de 64 (sessenta e quatro) bytes, sem perdas de pacotes.

3) O roteador Cisco 3745 possui MTBF (Mean Time Between Failures) superior a 50.000 (cinqüenta mil) horas.

4) O roteador Cisco 3745 permite a configuração de 1024 (mil e vinte e quatro) rotas estáticas.

5) A módulo de rede NM-1A-E3, compatível com o roteador Cisco 3745, possui interface compatível com o padrão ITU-T G.703.

6) O roteador Cisco 1751-V possui fonte de alimentação elétrica de 90 a 240 Volts com comutação automática e freqüencia de 60 (sessenta) Hertz.

7) A Cisco do Brasil recomenda, para o Edital 050/2003 da Empresa de Correios e Telégrafos, o uso o sistema operacional Pix OS versão 6.2 para os firewalls Cisco Pix 535 e Pix 525.

8) O firewall Cisco Pix 525 com a versão do sistema operacional Pix OS 6.2 possui capacidade de processamento superior a 350 Mbps em texto claro.

9) O sistema de detecção de intrusão IDS 4250 permite a detecção de ataques que utilizam recursos de detecção Whisker anti-IDS.

10) O sistema de detecção de intrusão IDS 4250 permite a detecção de Probin Attacks através das assinaturas de ataques do tipo Probe, como por exemplo Finger Probe, Apache/mod_ssl Worm Probe, SATAN Probe e Backdoor Probes em portas TCP ou UDP.

Atenciosamente,

Cisco do Brasil Ltda.
Sérgio Tsujioka
Representante Legal

CONFERIDO POR

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.3744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE:
001-SERGIO FUMIAKI ISUJIOKA
SAO PAULO, 23 DE JULHO DE 2003
EM TESTEMUNHO DA VERDADE
MARCIO ROBERTO TROFINO-ESC. AUTORIZ.
Total Custas.:*******2,07
Ear.:*137/1* DOC.S/V.ECONOMICO
Selo:1063*AA054805

FIRMA

1063AA054805

Doc.

REQS nº 03/2005 - CN
CPMI CORREIOS

Cisco do Brasil Ltda.
Av. Nações Unidas, 12.901 - 26°and
04578-903 - São Paulo – SP
Tel.: (011) 5508-9999
Fax: (011) 5505-9998
www.cisco.com

q796

Procuração

Outorgante: **Cisco do Brasil Ltda.**, com sede na cidade de São Paulo, Estado de São Paulo, na Avenida Nações Unidas, 12.901, 18°. e 26°. andares, CEP 04578-903, inscrita no CNPJ sob o n°. 00.028.666/0001-58, neste ato representada por seu gerente delegado, Sr. Carlos Carnevali, brasileiro, casado, engenheiro, portador da cédula de identidade RG n°. 3.500.054-SSP/SP, inscrito no CPF-MF sob o n°. 205.601.848-91, residente e domiciliado na Cidade de São Paulo-SP, com escritório na Cidade de São Paulo-SP, na Avenida Nações Unidas, 12.901, Torre Oeste, 26°. andar.

Outorgados: **Luis Carlos Araújo Moraes Rego Júnior**, brasileiro, engenheiro elétrico, portador da cédula de identidade RG n°. 6.953.526-7-SSP/SP, inscrito no CPF-MF sob o n°. 082.948.428-00, e **Sérgio Fumiaki Tsujioka**, brasileiro, técnico administrativo, portador da cédula de identidade RG n°. 4.639.759-0-SSP/SP, inscrito no CPF-MF sob o n°. 682.843.908-25, ambos residentes e domiciliados na Cidade de São Paulo-SP, com escritório na Cidade de São Paulo-SP, na Avenida Nações Unidas, 12.901, Torre Oeste,18°. andar.

Poderes: Pelo presente instrumento particular e nos termos do seu Contrato Social atualmente em vigor, a Outorgante nomeia e constitui os Outorgados seus bastante procuradores com poderes para individualmente (i) representar a Outorgante perante as repartições públicas federais, estaduais e municipais, entidades autárquicas e paraestatais, incluindo mas não limitando ao Banco Central do Brasil e às Juntas Comerciais, INSS, neles requerendo, assinado cartas, petições, formulários, documentos de câmbio, arquivar e retirar documentos; (ii) assinar contratos com empresas de utilidade pública e prestadores de serviços, incluindo mas não se limitando a contratos bancários e contratos de câmbio; (iii) representar a Outorgante em licitações, estando autorizado, para esse fim, a assinar documentos em benefício da Outorgante; (iv) interpor e responder recursos administrativos perante qualquer órgão da Administração Pública; (v) movimentar as contas bancárias em nome da Outorgante, assinar cheques e transferências, autorizar ordens de pagamento; e (vi) praticar todos os demais atos necessários ao bom e fiel cumprimento do presente mandato, mas sempre de total conformidade com as disposições e restrições contidas no Contrato Social da Outorgante. É vedado o substabelecimento no todo ou em parte da presente procuração.

Validade: A presente procuração vigorará de 03 de Janeiro de 2003 até **03 de Janeiro de 2004**, a menos que anteriormente revogada.

São Paulo, 19 de dezembro de 2002

Cisco do Brasil Ltda.
Carlos Carnevali
Gerente Delegado

RECEBIDO
RQS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1096

1º TABELIÃO DE NOTAS DE IBIRAPUERA
RECONHECE POR SEMELHANÇA 0001 FIRMAS DE:
CARLOS ROBERTO CARNEVALI
EM 19 DE DEZEMBRO DE 2002.
DA VERDADE

TABELIÃO DE IBIRAPUERA
São Paulo - Capital - Tel: 5505-8570
AUTENTICAÇÃO: ESTA CÓPIA REPROGRÁFICA CONFERE COM O ORIGINAL DA QUAL FOI EXTRAÍDA
Dou Fé!
21 JUL. 2003
SP,
Alcides Batista Correia - Escr. Aut.
Marcio Roberto Trevisan - Escr. Aut.
POR AUTENTICAÇÃO R$ 1,10

Marcio Roberto Trevisan
Escrevente Autorizado
RECONHECIMENTO DE FIRMA
1480AA525867

COM O SELO DE AUTENTICIDADE
Colégio Notarial do Brasil SP
CAPITAL
5505-8570
AUTENTICAÇÃO

BLACK BOX®
NETWORK SERVICES

São Paulo, 23 de julho de 2003.

A
EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS
BRASILIA/DF

Ref.: PREGÃO Nº050/2003 – CPL/AC
Objeto.: Locação e instalação de 162(cento e sessenta e dois) equipamentos de informática – novos de fábrica – incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme condições gerais e pauta de distribuição e especificações constantes dos ANEXOS 1-a e 1-B deste EDITAL.

DECLARAÇÃO DE SOLIDARIEDADE

Declaramos, na qualidade de fabricante, que a Itautec Informática S.A Grupo Itautec Philco , CNPJ nº 51.764.058/0001-42, é nosso revendedor autorizado e está apto a comercializar os equipamentos por nós produzidos, descritos abaixo:

KV138A	KV134A-R2	EHN151-0020	EHN382-0050	EHN383-0100
KV1301C-R2	KV131A-R2	KV1300C	KV1305C	KV1306C
KV140035	KV180035	EHN151-0020	RMK19A	EHN515-0050
EHN382-0100	EHN225-0100	KV140050		

Declaramos ainda :

a) nossa solidariedade para com a Itautec Informática S/A-Grupo Itautec quanto aos compromissos que esta venha a assumir perante a EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS;
b) que a Itautec Informática S/A- Grupo Itautec está apta a prestar assistência técnica, com uso de peças e componentes originais, bem como suporte aos produtos e equipamentos cotados;
c) que somos responsáveis solidários com a Itautec Informática S/A- Grupo Itautec, pelo perfeito cumprimento das exigências de garantia dos equipamentos, durante todo o seu prazo de vigência do contrato.
d) A Black Box do Brasil assegura que os referidos equipamentos são de linhas de produção continuada no período de 60 meses.

Carlos Cezar Fagan
Gerente de Vendas e Suporte
Black Box do Brasil Ltda

RQS nº 03/2005 - NT
CPMI - CORREIOS
Fls. Nº
Doc.

a794

SELENE CUBEROS PEREZ

TRADUTOR PÚBLICO

INGLÊS - PORTUGUÊS

Matr. JUCESP Nº 1695
C.C.M. 9.382.440-0

Rua Libero Badaró, 293 - 25º. Andar - São Paulo - SP – 01009-907
TEL.: 55 11 3188-5555 – Fax: 55 11 3188-5566

TRADUÇÃO Nº I-8533/02 LIVRO Nº 77 FOLHAS Nº 1

CERTIFICO E DOU FÉ, que me foi apresentado, nesta data, um documento redigido em idioma INGLÊS, com o fim de traduzi-lo para o PORTUGUÊS, o que faço em razão do meu ofício e nos termos seguintes:-.-

Project Management Institute [PMI - Instituto de Administração de Projetos]

Certifico que Claudia Fernanda Curcio satisfez todas as exigências estabelecidas e foi nomeada pelo Project Management Institute como Project Management Professional [PMP - Profissional de Administração de Projeto]. 1º de março de 2002 a 31 de dezembro de 2005.
Em testemunho do quê, subscrevemo-nos e selamos com o selo do Instituto.
Número da certificação: 47470.
Assinado: [assinatura ilegível].
Cargo: Presidente do Conselho de Diretores.
Assinado: [assinatura ilegível].
Cargo: Diretor Executivo.
[Consta o logotipo do Project Management Professional do PMI e o Selo Social do Project Management Institute, Inc.].
Propriedade do Project Management Institute.
[Verso].
© 2000 Project Management Institute, Inc. Todos os direitos reservados.
O "PMI" e o logotipo do PMI são serviços e marcas comerciais registradas nos Estados Unidos e em outros países; o "PMP" e o logotipo do PMP são marcas de certificação registradas nos Estados Unidos e em outros países; o "PMBOK", o "PM Network" e o "PMI Today" são marcas comerciais registradas nos Estados Unidos e em outros países; e o "Project Management Journal" e o "Building professionalism in project management" são marcas comerciais registradas do Project Management Institute, Inc.
Impresso nos Estados Unidos da América.
050-009-2000 (rev. 12/00).

NADA MAIS consta do documento a mim apresentado.
Conferi a tradução e dou fé.
O Tradutor Público e Intérprete Comercial.
São Paulo, 22 de Outubro de 2002.

SELENE CUBEROS PEREZ
TRADUTOR PÚBLICO JURAMENTADO

21º Tabelião de Notas
Reconheço por SEMELHANÇA a(s) firma(s) de: SELENE CUBEROS PEREZ

TABELIÃO DE NOTAS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1095
Doc.

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.º 33.372.251/0001-56, na condição de fabricante, declara que os racks IBM NetBay 42 Standard Rack e IBM NetBay 42 Expansion Rack possuem colunas de 2º. Plano e portas frontal, traseira e laterais removíveis, conforme item 7. RACK PARA EQUIPAMENTOS, sub-item 1 do Anexo 02 do Edital do Pregão n.º 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

15o CARTORIO DE NOTAS DE SAO PAULO
Rua da Gloria, 98 - Fone:(0XX11) 3105-9194\98
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
reco por SEMELHANCA 0001 FIRMA(S) DE:
ARMEN LUCIA TAVORA VIEIRA
AULO, 23 de JULHO de 2003.
INANTE:MIGUEL PERES JUNIOR
GO:ESCREVENTE AUTORIZADO.....
:.:#######2,07 Validado Por
bo:220595
PAGOS POR VERBA

Colegio Notarial do Brasil
FIRMA 1
1059AA009402

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1089
Doc. 79

DECLARAÇÃO

A empresa IBM Brasil Indústria, Máquinas e Serviços Ltda., CNPJ n.° 33.372.251/0001-56, na condição de fabricante, declara que os teclados ofertados suportam o padrão ABNT2, conforme item 3.4 SWITCH TIPO 4 (KVM), sub-item 3 do Edital do Pregão n.° 050/2003-CPL/AC.

Brasília - DF, 23 de Julho de 2003.

Carmem Távora Vieira
RG. 1451032-88 SSP-CE
Gerente de Unidade de Negócios
IBM Brasil Indústria, Máquinas e Serviços Ltda.

15o CARTORIO DE NOTAS DE SAO PAULO ###
Rua da Gloria, 98 - Fone:(0XX11) 3105-9194
VALIDO SOMENTE COM O SELO DE AUTENTICIDADE
eco por SEMELHANCA 0001 FIRMA(S) DE:
ARMEN LUCIA TAVORA VIEIRA
ULO, 23 de JULHO de 2003.
MANTE:MIGUEL PERES JUNIOR
SO:ESCREVENTE AUTORIZADO.....
.:###### 2,07 Digitado Por
o:220594
PAGOS POR VERBA

Colegio Notarial do Brasil - Seção SP
FIRMA 1
1059AA009401

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1100
Doc.

Aceco TI
Organização, Segurança e Continuidade

ACECO TI Ltda.
Av. Eng. Luiz Carlos Berrini, n.° 267 – Bloco B – 2° andar
CEP. 04571-010 – São Paulo - SP
CNPJ. 43.209.436/0002-89

Carta de Solidariedade

Ref: Edital do Pregão ECT No. 050/2003 – Objeto: locação e instalação de 162 (cento e sessenta e dois) equipamentos de informática – novos de fábrica - incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo.

Vimos, por meio desta, apresentar nossa solidariedade com a ITAUTEC Informática S/A – Grupo Itautec Philco. CNPJ: 51.764.058/0001-42, localizada na Rua Santa Catarina, n.° 1, Prédio 18, Parte, Tatuapé, São Paulo, SP, Brasil, no Edital supracitado, que estamos solidários a esta, garantindo o fornecimento dos seguintes produtos:

DESCRIÇÃO DOS PRODUTOS (citar marca e modelo)

Intervenções necessárias

Fornecimento de expansão do sistema de detecção precoce de incêndio, para complementação do sistema em virtude do complemento do sistema de climatização da Sala de Segurança;

Integração dos novos equipamentos aos sistemas de detecção precoce de incêndio , controle e monitoramento ambiental existentes, de modo a manter as características e performance de atuação sem prejuízos ao sistema já instalado.

Quadros gerais de distribuição dos No-Breaks, Barramento Seguro (QDX e QDY)

Estes quadros serão complementados com a instalação de novos disjuntores para alimentação de novos painéis de distribuição interna da sala de segurança física, no mesmo padrão e funcionalidade dos atuais.

6 Quadros auto portantes tipo plug-in da Sala Cofre: (QdiX2 , QdiY2) em São Paulo e (QdiX2, QdiY2 , QdiX3 e QdiY3) em Brasília.

Os quadros a serem instalados, seguirão o mesmo padrão existente, dotados de disjuntores extraíveis (plug-in) com tampa transparente em policarbonato.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1101
Doc.

Serão contemplados um total de 108 (cento e oito) circuitos duais, totalizando 216 (duzentos e dezesseis) pontos elétricos no ECT Brasília e 65 (sessenta e cinco) circuitos duais, totalizando 130 (cento e trinta) pontos elétricos no ECT São Paulo.

Todos os quadros seguirão o padrão dos quadros atuais como fabricante e linha de disjuntores, medições e outras características.

Sistema de Eletrocalhas / Leito Aramado

Serão utilizadas eletrocalhas existentes para a execução da interligação entre os quadros QDX e QDY.

Para a infra estrutura sob o piso elevado das salas serão utilizados leitos aramados em inox, com os devidos acessórios de derivação e fixação e identificações seguindo o padrão existente.

Sistema de Cabeamento lógico

São Paulo

Cabeamento Horizontal UTP: instalação de 6000 metros de UTP 4 pares cat. 6 para atender os 180 pontos estruturado, sendo que os 180 pontos estão sendo considerados para atender as estações de trabalho e equipamentos dentro da sala cofre. Esses 180 pontos serão distribuídos de forma horizontal para atender cada estação de trabalho com 02 pontos, possibilitando serviços de (Dados , Voz, Imagem etc.) em cada ponto, esses cabos seguirão por leitos aramados até os Racks a serem instalados conforme o lay out a ser definido.

Conectores UTP: Instalação de 180 conectores RJ-45 fêmea cat. 6 para terminação nas extremidades dos cabos UTP 4 pares do Cabeamento Estruturado .

Surface Box : Fornecimento e instalação de 90 Surface Box com duas 2 posições, para a instalação e identificação dos conectores RJ-45 fêmea nas estações de trabalho.

Patch Panel UTP: Fornecimento e instalação de 8 patch panels 19" com 24 portas cat. 6 dentro dos Racks a serem instalados, para terminação dos cabos UTP 4 pares provenientes das estações de trabalho.

Patch Cords UTP: Fornecimento e instalação de 180 patch cords de 1,5 metros para conexão de serviços de dados e voz nos Racks, referidos acima.

Fornecimento e instalação de 180 patch cords de 3,0 metros para conexão de serviços de dados nas estações de trabalho, referidos acima.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1102
Doc.

Aceco TI
Organização, Segurança e Continuidade

Organizador Horizontal: Fornecimento e instalação 20 organizadores horizontais de 19"x 1U de altura, para organização dos patch cords nos Racks.

Cabeamento Ópticos: Serão disponibilizados um total de 128 fiber channel , com cordão dúplex SC/SC MM com 3 metros do SW até distribuidor óptico e 27 metros do distribuidor óptico até o equipamento para atender as nessecidades de acréscimo no site ETC São Paulo.

Testes e Identificações: Execução de medições para efetuar testes em todos os cabos UTP cat 6 e Ópticos , com emissão de relatórios dos resultados e instalação de etiquetas para identificação de todo o cabeamento instalado.

Brasília

Cabeamento Horizontal UTP: instalação de 12000 metros de cabos UTP 4 pares cat 6 para atender os 400 pontos estruturado, sendo que os 400 pontos estão sendo considerados para atender as estações de trabalho e equipamentos dentro da sala cofre. Esses 400 pontos serão distribuídos de forma horizontal para atender cada estação de trabalho e equipamentos com 02 pontos, possibilitando serviços de (Dados Voz, Imagem etc.) em cada ponto, esses cabos seguirão por leitos aramados até os Racks a serem instalados conforme o lay out a ser definido.

Conectores UTP: Instalação de 400 conectores RJ-45 fêmea cat. 6 para terminação nas extremidades dos cabos UTP 4 pares do Cabeamento Estruturado nas estações de trabalho.

Surface Box : Fornecimento e instalação de 200 Surface Box com 2 posições, para a instalação e identificação dos conectores RJ-45 fêmea nas estações de trabalho.

Patch Panel UTP: Fornecimento e instalação de 17 patch panels 19" com 24 portas cat. 6 dentro dos Racks a serem instalados, para terminação dos cabos UTP 4 pares provenientes das estações de trabalho.

Patch Cords UTP: Fornecimento e instalação de 400 patch cords de 1,5 metros para conexão de serviços de dados e voz nos Racks, referidos acima.

Fornecimento e instalação de 400 patch cords de 3,0 metros para conexão de serviços de dados nas estações de trabalho, referidos acima.

Organizador Horizontal: Fornecimento e instalação de 40 organizadores horizontais de 19"x 1U de altura, para organização dos patch cords nos Racks.

Cabeamento Óptico: Serão disponibilizando um total de 256 fiber channel com cordão duplex SC/SC MM com 3 metros do SW até o distribuidor óptico e 27 metros do

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls nº 1101
Doc.

distribuidor óptico até os equipamentos para atender as nessecidades no site do ECT Brasília.

Testes e Identificações: Execução de medições para efetuar testes em todos os cabos UTP e Ópticos instalados, com emissão de relatórios dos resultados e instalação de etiquetas para identificação de todo o cabeamento instalado.

Todas as alterações nos projetos, quando da execução dos serviços, serão assinaladas em AS-BUILT.

Sistema de Climatização

Para o site de Brasília será necessário o complemento do sistema de climatização existente.

Serão fornecidos 2 novos equipamentos de climatização, de mesmas características e potência dos demais já instalados na Sala de Segurança - modelo 24UW.

Adicionalmente atestamos:

a) nossa solidariedade com a ITAUTEC no âmbito dos produtos acima listados, quanto aos compromissos por ela assumidos na licitação supra-citada;
b) Que a ACECO TI está apta a prestar assistência técnica para ITAUTEC, com o uso de peças e comprovantes originais, bem como suporte aos produtos cotados.
c) Nossa responsabilidade solidária com a ITAUTEC pelo perfeito cumprimento das exigências de garantia dos produtos, durante o todo o prazo de vigência do Contrato.

CONFERIDO POR

São Paulo, 23 de julho de 2003

JOÃO LUCIO DOS REIS Fº
Diretor
ACECO TI Ltda.

30.CARTORIO REGISTRO CIVIL IBIRAPUERA
AV.Nova Independencia,51 Fone: 5506.5744
VALIDO SOMENTE COM SELO DE AUTENTICIDADE
RECONHECO POR SEMELHANCA 0001 FIRMAS DE:
0001-JOAO LUCIO DOS REIS FILHO
SAO PAULO, 23 DE JULHO DE 2003.
EM TESTEMUNHO DA VERDADE
ALCIDES BATISTA CORREIA-ESP. AUTORIZ.
Total Custas.:******2,07
Car.:1338166 DOC.S/V.ECONOMICO
Selo:1063XAA057077

Colegio Notarial do Brasil SP
Escrevente Autorizado
FIRMA RECONHECIDA
1063AA057077

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1104
Doc.

Itautec

a787

À
Empresa Brasileira de Correios e Telégrafos – ECT
Comissão Permanente de Licitação da Administração Central - CPL/AC
SBN – Quadra 01 – Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília - DF

Ref.: Pregão 050/2003 – CPL/AC
Data: 24/07/2003 às 9:00 Horas

DECLARAÇÃO DE RESPONSABILIDADE DOS COMPONENTES DE TERCEIROS E DISPONIBILIDADE DE CENTRAL DE ATENDIMENTO

A Itautec Informática S/A – Grupo Itautec Philco, CNPJ Nº 51.764.058/0001-42, pelo seu Representante Legal Sr.(a) Jorge Ítalo Dimatteu Telles, portador(a) da Carteira de Identidade nº 636.695 – SSP/DF e CPF nº 292.880.961-91, declara que o fornecimento de equipamentos/softwares ou prestação de serviços por terceiros, constantes da nossa proposta, não diminui, em hipótese alguma, a nossa total responsabilidade pelo perfeito e completo funcionamento do objeto do Edital do Pregão nº 050/2003-CPL/AC.

Declaramos, ainda, de que vamos dispor, no prazo máximo de 20 (vinte) dias da assinatura do Contrato, e central de atendimento telefônico com discagem gratuita e/ou internet, para processo de recepção, qualificação, controle e solução dos chamados de manutenção corretiva.

Atenciosamente,

Brasília – DF, 24 de julho de 2003.

Itautec Informática S.A
Grupo Itautec Philco
Jorge Ítalo Dimatteu Telles
Representante de Marketing

Itautec Informática S.A.
Grupo Itautec Philco
Raimundo Carlos Pereira
Gerente Comercial

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1105
Doc

Itautec

À
Empresa Brasileira de Correios e Telégrafos – ECT
Comissão Permanente de Licitação da Administração Central - CPL/AC
SBN – Quadra 01 – Bloco "A" – Sobreloja – Ed. Sede ECT
Brasília - DF

Ref.: Pregão 050/2003 – CPL/AC
Data: 24/07/2003 às 9:00 Horas

Esclarecimentos Técnicos

A Itautec Informática S/A – Grupo Itautec Philco, CNPJ Nº 51.764.058/0001-42, pelo seu Representante Legal Sr. Jorge Ítalo Dimatteu Telles, portador da Carteira de Identidade nº 636.695 – SSP/DF e CPF nº 292.880.961-91, informa abaixo os telefones dos técnicos que poderão esclarecer possíveis dúvidas ou questionamentos referentes ao produtos ofertados na sua proposta referente ao objeto do Edital do Pregão nº 050/2003-CPL/AC:

1. Jéferson Moia – (0xx11)-9613-201 3; Carlos Jr – (0xx61) 9985-2954 – Servidor Intel Tipo 01, Servidor Intel Tipo 02, Servidor Intel Tipo 03
2. César Maciel – (0xx31)-9957-5096; Henrique Von – (0xx61) 9987-2894 – Servidor Risc Tipo 01
3. Carlos Pane – (0xx11) 9619-6934 – Switch Tipo 01, Switch Tipo 02, Switch Tipo 05, Roteador Tipo 01, Roteador Tipo 02, Servidor de Segurança Lógica Tipo 01, Servidor de Lógica Tipo 02, Servidor de Segurança Lógica Tipo 01, Servidor de Segurança Lógica 02, Servidor de Detecção de Intrusão
4. Mauro Galindo – (0xx61)921-8532; Heric – 0xx61-8116-3351- Switch Tipo 03, Unidade de Backup Robotizado
5. Douglas Fernandes – (0xx11) 9619-6846 – Switch Tipo 04

Atenciosamente,

Brasília – DF, 24 de julho de 2003.

Itautec Informática S.A
Grupo Itautec Philco
Jorge Ítalo Dimatteu Telles
Representante de Marketing

Itautec Informática S.A.
Grupo Itautec Philco
Raimundo Carlos Pereira
Gerente Comercial

ECT - PRES - 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1106
Doc.

SELENE CUBEROS PEREZ

TRADUTOR PÚBLICO

INGLÊS - PORTUGUÊS

Matr. JUCESP Nº 1695
C.C.M. 9.382.440-0

Rua Libero Badaró, 293 - 25º. Andar - São Paulo - SP – 01009-907
TEL.: 55 11 3188-5555 – Fax: 55 11 3188-5566

0785

TRADUÇÃO Nº I-8533/02 LIVRO Nº 77 FOLHAS Nº 1

CERTIFICO E DOU FÉ, que me foi apresentado, nesta data, um documento redigido em idioma INGLÊS, com o fim de traduzi-lo para o PORTUGUÊS, o que faço em razão do meu ofício e nos termos seguintes:-.-

Project Management Institute [PMI - Instituto de Administração de Projetos]

Certifico que Claudia Fernanda Curcio satisfez todas as exigências estabelecidas e foi nomeada pelo Project Management Institute como Project Management Professional [PMP - Profissional de Administração de Projeto].
1º de março de 2002 a 31 de dezembro de 2005.
Em testemunho do quê, subscrevemo-nos e selamos com o selo do Instituto.
Número da certificação: 47470.
Assinado: [assinatura ilegível].
Cargo: Presidente do Conselho de Diretores.
Assinado: [assinatura ilegível].
Cargo: Diretor Executivo.
[Consta o logotipo do Project Management Professional do PMI e o Selo Social do Project Management Institute, Inc.].
Propriedade do Project Management Institute.
[Verso].
© 2000 Project Management Institute, Inc. Todos os direitos reservados.
O "PMI" e o logotipo do PMI são serviços e marcas comerciais registradas nos Estados Unidos e em outros países; o "PMP" e o logotipo do PMP são marcas de certificação registradas nos Estados Unidos e em outros países; o "PMBOK", o "PM Network" e o "PMI Today" são marcas comerciais registradas nos Estados Unidos e em outros países; e o "Project Management Journal" e o "Building professionalism in project management" são marcas comerciais registradas do Project Management Institute, Inc.
Impresso nos Estados Unidos da América.
050-009-2000 (rev. 12/00).

NADA MAIS consta do documento a mim apresentado.
Conferi a tradução e dou fé.
O Tradutor Público e Intérprete Comercial.
São Paulo, 22 de Outubro de 2002.

24 JUL 2003

21º Tabelião de Notas
Reconheço por SEMELHANÇA a(s) firma(s) de: SELENE CUBEROS PEREZ

SELENE CUBEROS PEREZ
TRADUTOR PÚBLICO JURAMENTADO

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 107
Doc.

Doc.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

ITAUTEC INFORMÁTICA S/A – MANUAL VOLUMES 1 E 2

2003
PASTA 16

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1103
Doc.

Itautec

ECT
11 053
Paula

ANEXO 3

CATÁLOGOS, MANUAIS E OUTROS DOCUMENTOS TÉCNICOS

VOLUME 1

CONTEÚDO:

- MANUAL 1
- MANUAL 2
- MANUAL 3
- MANUAL 4
- MANUAL 5
- MANUAL 6
- MANUAL 7

SCS Q. 01 Bloco "F" 11º Andar – Ed. Camargo Corrêa – Brasília-DF CEP: 70397-900 - Fone: (61) 323-3031 Fax: (61) 226-1251

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1109
Doc. 3698

11052
Paula

Manual 1

IBM TotalStorage TM
SAN Swtich M12

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1110
Doc. 3698

Core fabric switch supports highly scalable fabrics for large enterprise SANs

11 051 Paula CPI

IBM TotalStorage™ SAN Switch M12

High port density packaging saves space

Highlights

- ***Designed to provide superior performance with up to 2 Gbit/sec throughput and Inter-Switch Link (ISL) Trunking with aggregate speed up to 8 Gbit/sec***
- ***Enterprise-level scalability and high availability when deployed with dual redundant core/edge fabrics capable of attaching thousands of devices***
- ***Scalable from one 32-port swtich to two 64-port switches***
- ***Broadest range of IBM open server and storage device attachment including fabric, public loop and private loop with QuickLoop enabled edge switches***
- ***Space saving Small Form-Factor Pluggable (SFP) transceivers with up to 128-ports of Fibre Channel connectivity in 14U enclosure***
- ***Advanced fabric services such as end-to-end performance monitoring***
- ***Multiple SAN management options include IBM TotalStorage SAN Switch Specialist, Fabric Manager V3 and open fabric interfaces for centralized management of large core/edge fabrics***

IBM TotalStorage Enterprise SAN products

The IBM TotalStorage enterprise Storage Area Network (SAN) products create a high-speed, interconnected switch fabric of centrally managed, multi-vendor heterogeneous servers and storage systems. An enterprise SAN built upon IBM SAN technology can help companies derive greater value from their business information by supporting improved IT resource management and information sharing across the enterprise.

IBM TotalStorage SAN Switch M12

The IBM TotalStorage SAN Switch M12 (M12 Switch) provides 2 Gbit Fibre Channel capability and performance and advanced functions to address demands for improved security, performance and manageability as the SAN fabric grows to include thousands of devices. It is based on next-generation switch technology that is designed to help full interoperable with other IBM TotalStorage SAN Switches. You can configure scalable solutions that address your needs for high performance and reliability for environments ranging from small workgroups to very large, integrated enterprise SANs.

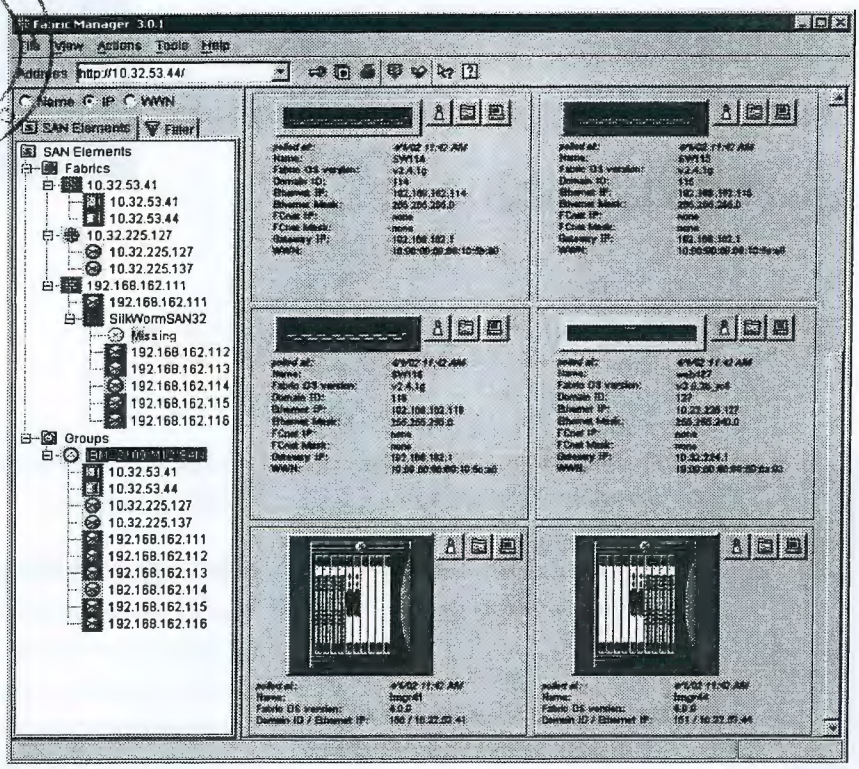
Industry-standard Fibre Channel

The M12 Switch is designed to provide Fibre Channel connectivity to:

Servers:

- *IBM @server pSeries and selected RS/6000 servers (for the most current list of supported servers and storage, visit ibm.com/storage/FCSwitch)*
- *IBM @server xSeries and selected Netfinity servers*
- *Other Intel®-based servers with Windows NT®/2000*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1111
Doc. 3698



SAN Switch Specialist Switch View

Storage Systems

- *IBM Enterprise Storage Server®*
- *IBM FAStT Storage Server® family*
- *IBM 3590 Tape Subsystems and 3494 Tape Libraries*
- *IBM 3583 and 3584 Ultrium Tape Libraries*

SAN Switches

- *IBM TotalStorage SAN Switch F16 and F08 (F16 and F08 Switches)*
- *IBM TotalStorage SAN Switch S16, S08 (S16 and S08 Switches) and IBM TotalStorage SAN Managed Hub*

The M12 Switch supports the interconnection of multiple IBM SAN Switches. The interconnection of IBM and compatible (Brocade® SilkWorm® 2400, 2800, 3200, 3800 and 12000) switches can support the creation of a scalable, dual redundant core-to-edge SAN fabrics that can support high performance, scalability, and fault tolerance required e-business applications and enterprise storage management applications—such as storage consolidation, data protection, disaster tolerance and data sharing.

IBM TotalStorage SAN Switches

IBM S08 and S16 Switches are designed to support ANSI-standard Fibre Channel protocol at 1 Gbit/sec. The M12 Switch is built upon a next-generation switch technology that provides link speeds of 1 and 2 Gbit/sec. Each port supports either 100MB/sec or 200MB/sec, full-duplex data transfers. Auto-sensing ports are capable of automatically negotiating to the highest speed supported by the attached server, storage or switch.

The M12 Switch is suited for disaster tolerance solutions such as remote tape vaulting and remote disk mirroring. M12 Switches can provide up to twice the throughput of S16 Switches. This performance capability can be used to either reduce the number of expensive extended distance ISL connections or to improve the performance with the same number of connections.

M12 Switches can be combined with F16 and F08 Switches to provide fabrics up to twice the performance of S16 and S08 Switch fabrics. Customers can deploy M12 Switches that are ready to exploit the performance potential of newer servers and storage devices with 2 Gbit/sec capabilities.

M12 Switches can be used to expand an existing core-to-edge SAN fabric infrastructure. As M12 Switches are added to the core, installed F16, S16 and S08 Switches can be migrated to the edge. This approach helps support scalable network growth in a modular, effective and non-disruptive manner while customers continue to derive benefit from installed switches.

Common SAN Switch functions and features

IBM TotalStorage SAN Switches include universal ports that can automatically determine the port type when connected to a fabric port (F_port), fabric loop port (FL_port) or expansion port (E_port). Fabric services include automatic self-discovery of new devices and dynamic path selection based upon Fabric Shortest Path First (FSPF) which is designed to select the most efficient routing in a SAN fabric. A mixture of shortwave and longwave ports can be configured. The core fabric switch is designed to provide improved switch availability with hot swappable components that can be replaced or upgraded without interrupting network operations. Components include switch modules, redundant power supplies, cooling systems and processors and support for non-disruptive software upgrades.

Common firmware functions and features

The common IBM SAN Switch firmware simplifies SAN fabric expansion. Standards-based Management Server and Simple Name Server support in-band discovery of SAN fabric changes. Management access of SNMP information is provided via an external Ethernet interface or in-band over a Fibre Channel link through a single fabric connection.

Device-level zoning of the SAN fabric enables an administrator to create separate segments or zones within the SAN fabric to separate different application servers and devices in heterogeneous SAN environments. Zones may be dynamically created and changed from any switch in the fabric. Basic security functions such as hardware-enforced zoning are standard.

Extended Fabric Activation extends SAN fabrics beyond the Fibre Channel standard 10 km. This enables high performance applications over extended distances for storage consolidation, data protection, disaster tolerance and data sharing. ISLs using extended longwave transceivers, Fibre Channel repeaters and Dense Wave Division Multiplexing (DWDM) devices can provide Metropolitan Area Network (MAN) connectivity distances. Extended Fabrics Activation helps optimize switch buffering to support high gateway switch ISL performance.

Remote Switch Activation extends the distance of SAN fabrics by enabling two Fibre Channel switches to interconnect over an ATM Wide Area Network (WAN). With this feature, one can stage and manage data transfers across a pair of Fibre Channel switches connected to a pair of CNT Open System Gateways.

QuickLoop enables servers with Fibre Channel Arbitrated Loop (FC-AL) private loop Host Bus Adapters (HBAs) to communicate with FC-AL storage devices through IBM SAN Switches. The M12 Switch does not provide QuickLoop capability. However, IBM SAN Switches with QuickLoop enabled may be used to attach private loops devices to M12 Switches.

M12 Switch configuration options

A single switch with two 16-port switch blades and thirty-two universal ports, is scalable up to two 64-port switches, each with four switch blades. A mixture of shortwave and longwave ports can be configured by adding up to 128 SFP optical transceivers.

Inter-Switch Link (ISL) Trunking, a standard feature, enables as many as four Fibre Channel links between next-generation switch technology M12, F16 and F08 Switches to be combined to form a single logical ISL with an aggregate speed of up to 8 Gbit/sec. These high-speed trunks help optimize bandwidth utilization and enhance availability.

Load balancing can help balance the load across all of the ISLs through trunking. This enables administrators to focus on overall network performance rather than individual link congestion from multiple higher performance devices sharing a single link. Administrators need only to monitor the trunk performance rather than specific devices being routed across it. Increased network reliability and performance is supported because failed links do not require rerouting of traffic.

End-to-end performance monitoring

Next-generation switching technology enables Frame Filtering, which is based upon additional information in several fields in both the packet header and payload. Frame Filtering enables new intelligent fabric services such as end-to-end performance analysis.

S08 and S16 Switches provide performance information at the switch or port level. M12 Switches with Frame Filtering provide detailed information at the frame level. This information can be used to monitor performance end-to-end across the entire core-to-edge SAN fabric—from a specific server to a specific storage device port.

Performance Monitoring, a standard feature, provides support for Frame Filtering-based Performance Monitoring tools for enhanced end-to-end performance monitoring. As core-to-edge SAN fabrics scale up to thousands of devices, ISL Trunking and Frame Filtering can help to simplify storage management and reduce the overall cost of the storage infrastructure.

C36 Cabinet options

The C36 Cabinet is based upon a standard 19-inch rack, and offers 36U vertical space. It is specifically designed to support two M12 Switches with two power distribution units, each with three power outlets. A Ruggedized Rack feature provides enhanced rigidity and stability for locations with earthquake concerns.

Open fabric management

IBM SAN Switch management framework is designed to support the widest range of solutions—from the very small workgroup SANs up to very large enterprise SAN fabrics with thousands of devices. Small SANs require rapid deployment and plug-and-play simplicity. Very large SAN fabrics require centralized management and automated administration. IBM SAN Switch

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1112
Doc. 3698

IBM TotalStorage SAN Switch M12 at a glance

Physical characteristics	M12 Switch	C36 Cabinet
Height	61.24 cm/24.11 in (14U)	180.4 cm/71.0 in (36U)
Width	43.74 cm/17.22 in	64.4 cm/25.4 in
Depth	74.20 cm/29.20 in	109.8 cm/43.3 in
Weight (fully populated)	113 kg/248 lb	One M12 357 kg/784 lb Two M12s 470 kg/1032 lb
Operating environment		
Temperature	0° to 40 ° C/32° to 104° F	10° to 40 ° C/50° to 104° C
Relative humidity	20% to 85% at 40° C/104° F	8% to 80% at 40° C/104° F
Power requirements		
Power range	180 to 264 VAC, 47 to 63 Hz	200 to 240 VAC, 50-60 Hz

Product numbers

2109 M12—IBM TotalStorage SAN Switch M12, a 32-port core fabric switch with enclosure includes four power supplies, three fans, two control processors and two 16-port, 2 Gb switch blades. The base configuration includes Fabric OS Version 4.0, IBM SAN Switch Specialist, Advanced Zoning, FabricWatch, ISL-Trunking, Performance Monitoring and space for two 64-port switches.
FC 2310—M12 Shortwave SFP transceiver
FC 2320—M12 Longwave SFP transceiver
FC 3216—16 Port Switch Blade

Fiber Optic Cables:
FC 5301—M12 Fiber cable, LC/LC, multimode optical, 50.0u, 1 meters
FC 5305—M12 Fiber cable, LC/LC, multimode optical, 50.0u, 5 meters
FC 5325—M12 Fiber cable, LC/LC, multimode optical, 50.0u, 25 meters
FC 5371—M12 Fiber LC/SC (male/female) coupling cable, multimode optical, 50.0u, 1 meters
FC 5372—M12 Fiber LC/SC (male/female) coupling cable, multimode optical, 50.0u, 2 meters

Advanced Fabric Features:
FC 7301—Fabric Manager V3
FC 7602—Remote Switch Activation
FC 7603—Extended Fabric Activation

2109 C36—IBM TotalStorage SAN Cabinet C36, 19-inch rack with 36U space, designed to support two M12 Switches with two power distribution units, each with three power outlets.
FC 6080—Ruggedized Rack

management options include a browser-based IBM TotalStorage SAN Switch Specialist, Fabric Manager V3 and open standards-based interfaces to enterprise SAN managers.

IBM TotalStorage SAN Switch Specialist is designed to provide a comprehensive set of management tools that support a Web browser interface for flexible, easy-to-use integration into existing enterprise storage management structures. The Switch Specialist supports security and data integrity by limiting (zoning) host system attachment to specific storage systems and devices.

Fabric Watch is a standard function on M12, F16, F08 (Full-Fabric), S16* and S08* Switches. Fabric Watch threshold monitoring tracks the health of switches and SAN fabric. Fabric Watch monitors fabric resources, port traffic, switch environmental values and operational values for GigaBit Interface Converters (GBIC) and optical transceivers. This information is accessible from the Switch Specialist. When used with M12 Switches, the Specialist provides an easy-to-use interface to intelligent fabric features such as end-to-end performance monitoring and ISL Trunking.

Fabric Manager V3 provides a Java-based application that can simplify management of a complex, multiple switch fabrics. IBM SAN Switch Specialist and Fabric Manager work together on the same management server which can be attached to any switch in the core/edge fabric. It may also manage up to eight separate fabrics. Fabric Manager requires a Windows NT/2000 or Sun Solaris 7 server with a Netscape or Internet Explorer web browser.

Enterprise SAN fabric management

Fabric Watch can send alerts to enterprise SAN fabric management software from vendors such as Computer Associates, Hewlett Packard, Tivoli, and VERITAS. Brocade Fabric Access Layer API server agents are available on IBM SAN Switches. Only a single connection to the fabric is required to access any switch or fabric-wide resource.

For more information

For more information, contact your IBM representative or IBM Business Pa[illegible]r. Or visit **ibm.com**/storage/FCSwitch.

© International Business Machines Corporation 2002

IBM Corporation
Storage Systems Group
5600 Cottle Road
San Jose, CA 95193

Produced in the United States of America
05-02
All Rights Reserved

* Models S08 and S16 shipped after March 23, 2001.

IBM and the IBM logo, Enterprise Storage Server, @server, Magstar, Netfinity, RS/6000, and S/390 are registered trademarks and iSeries, pS[illegible] TotalStorage, xSeries, and zSeries are trad[illegible] International Business Machines Corporation.

Windows 2000 and Windows NT are trademarks of Microsoft Corporation in the United States, other countries or both. UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

G225-6946-01

FCT
11.047
Paula

Manual 02

IBM TotalStorage TM
SAN Fibre Channel Switch 2109 M12

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 113
3698
Doc.

IBM TotalStorage ™ SAN Fibre Channel Switch 2109 Model M12

IBM Storage and Server Interoperability Matrix

Last update: Jun. 18, 03

© Copyright International Business Machines Corporation 1999, 2003. All rights reserved.

The information provided in this document is provide "AS IS" without warranty of any kind, including any warranty of merchantability, fitness for a particular purpose, interoperability or compatibility. IBM's products are warranted in accordance with the agreements under which they are provided.

Unless otherwise specified, the product manufacturer, supplier, or publisher of non-IBM products provides warranty, service, and support directly to you. IBM makes no representations or warranties regarding non-IBM products.

The inclusion of an IBM or non-IBM product on an interoperability list is not a guarantee that it will work with the designated IBM storage product. In addition, not all software and hardware combinations created from compatible components will necessarily function properly together. The following list includes products developed or distributed by companies other than IBM. IBM does not provide service or support for the non-IBM products listed, but does not prohibit them from being used together with IBM's storage products. During problem debug and resolution, IBM may require that hardware or software additions be removed from the IBM product to provide problem determination and resolution on the IBM-supplied hardware/ software. For support issues regarding non-IBM products, please contact the manufacturer of the product directly. IBM does not warrant either functionality or problem resolution of any non-IBM products.

This information could include technical inaccuracies or typographical errors. IBM does not assume any liability for damages caused by such errors as this information is provided for convenience only; the reader should confirm any information contained herein with the associated vendor.

Changes are periodically made to the content of the document. These changes will be incorporated in new editions of the document. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this document at anytime without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1111
Doc. 3698

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX	iSeries	S/390 Parallel Enterprise Server
AS/400	Micro Channel	SP
DYNIX	Multiprise	TotalStorage
DYNIX/ptx	Netfinity	Versatile Storage Server
e (logo)	NUMA-Q	VM/ESA
Enterprise Storage Server	OS/390	VSE/ESA
ESCON	OS/400	xSeries
ES/9000	PTX	z/OS
FICON	pSeries	zSeries
FlashCopy	Redbooks	z/VM
IBM	RS/6000	
IBM logo	S/390	

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

E C T
11.044
fls

Table of Contents

ESS
FAStT
Tape

Notes:

1. **Firmware** version **4.1.0** or later and Fabric Manager **4.0** are recommended.
2. **Reference Information.**
3. **Advanced Security Feature** is available with firmware version 4.1.0 or later.
4. Secure Fabric OS - **Field Upgrade Process**. **(Hints and Tips).**
5. SAN Fibre Channel Switch 2109 Model M12 **Data Sheet** (pdf).
6. Both tape and disk attached to the same HBA are not recommended.
7. We do not recommend attaching the NAS 300G to an **unzoned** switch configuration.
8. Planned availability dates represent current estimates and are subject to change or withdrawal at any time without notice.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1115
Doc. 3698

ESS Connectivity

See **IBM TotalStorage Enterprise Storage Server Interoperability Matrix** for Licensed Internal Code (LIC) level.

IBM pSeries, RS/6000 and RS/6000-SP Servers

Description	Operating Systems	Additional Information

IBM TotalStorage Enterprise Storage Servers
IBM 2105 Model
• F10/F20
• 800
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2 [1]
	
	HACMP [2]
	PSSP [2]
		Available
		
		Enterprise Storage Server Interoperability matrix
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.

[1] Planned availability is 2Q03 for RS/6000-SP with AIX 5.2.
[2] See **ESS** Interoperability matrix for **AIX, HACMP, PSSP, and SDD** support information.

11042 Paula

IBM xSeries, Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Enterprise Storage Servers **IBM 2105 Model** • F10/F20 • 800	**Microsoft Windows NT** • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server • Datacenter Server	Available **Enterprise Storage Server** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Novell Netware • 5.1 • 6.0	Available
	Red Hat Linux • 7.1 • 7.2 • 7.3 **Red Hat Linux Advanced Server** • 2.1 **SuSE Linux** • 7.2 • 7.3 **SuSE Linux Enterprise Server (SLES)** • 7 • 8	Available
	IBM TotalStorage Network Attached Storage 300G	Available

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1116
Doc. 3698

SUN microsystems Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Enterprise Storage Servers **IBM 2105 Model** • F10/F20 • 800	**Solaris** • 2.6 • 7 • 8 • 9 [3]	Available **Enterprise Storage Server** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
IBM TotalStorage Enterprise Storage Servers **IBM 2105 Model** • F10/F20 • 800	**HP-UX** • 11.0 • 11i	Available **Enterprise Storage Server** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

[3] Solaris 9 is not supported SDD at this time.

11.040 Paula

FAStT Connectivity

1 We do not recommend attaching the **IBM FAStT** on the same Intel server as the **TotalStorage Enterprise Storage Server**. Both devices may be attached to the same switch.

2 For the most current supported **HACMP, PSSP, GPFS/RVSD** configurations see the config files posted on:
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt900downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt700downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt600downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt500downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt200downloads

3 **GPFS** Linux supported on selected **xSeries** servers running RH 7.2, 7.3 or SuSE Linux Enterprise Server 7 or 8. Refer to the **IBM** Linux and **eServer** Cluster support pages.
- http://ibm.com/servers/eserver/clusters
- http://ibm.com/linux

IBM pSeries, RS/6000 and RS/6000 SP Servers

Description	Operating Systems	Additional Information

IBM TotalStorage Storage Servers
• FAStT900
• FAStT600
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2
	
	HACMP, PSSP (see note #2 page 7)
		Available
		
		IBM TotalStorage FAStT Storage Interoperability matrix
		
		IBM Server Proven Interoperability matrix
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 111
3698
Doc.

IBM xSeries, Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT900** • **FAStT600**	**Microsoft Windows NT** • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Novell Netware • 6.0	Available
IBM TotalStorage Storage Servers • **FAStT900**	**Red Hat Linux Advanced Server** • 2.1 **SuSE Linux Enterprise Server (SLES)** • 7 • 8	Available
IBM TotalStorage Storage Servers • **FAStT600**	**Red Hat Linux Advanced Server** • 2.1 **SuSE Linux Enterprise Server (SLES)** • 8	Available

E.C.T. 11.038 Paula

SUN microsystems Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT900** • **FAStT600**	**Solaris** • 2.6 • 7 • 8	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT900** • **FAStT600**	**HP-UX** • 11.0 • 11i	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 1118
3698
Doc.

IBM pSeries, RS/6000 and RS/6000 SP Servers

Description	Operating Systems	Additional Information

IBM TotalStorage Storage Servers
• **FAStT700**
• **FAStT500**
• **FAStT200**
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2
	
	HACMP, PSSP (see note #2 page 7)
		Available
		
		IBM TotalStorage FAStT Storage Interoperability matrix
		
		IBM Server Proven Interoperability matrix
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.

ECT 11.036 Paula COL-AC

IBM xSeries and Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT700** • **FAStT500** • **FAStT200**	**Microsoft Windows NT** • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Novell Netware • 5.1 • 6.0	Available
	Red Hat Linux • 7.1 • 7.2 • 7.3 **Red Hat Linux Adv. Server** • 2.1 **SuSE Linux** •7.3 **SuSE Linux Enterprise Server** • 7 • 8 **Turbo Linux** • 7.0	Available
	IBM TotalStorage Network Attached Storage 300G	Available

RQS nº 03/2005 - CN CPMI CORREIOS Fls. Nº 1119 3698 Doc.

SUN microsystems Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT700** • **FAStT500** • **FAStT200**	**Solaris** • 2.6 • 7 • 8	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT700** • **FAStT500** • **FAStT200**	**HP-UX** • 11.0 • 11i	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

11.034 Paula

TAPE Connectivity

AVOID DYNAMIC ZONING CHANGES
As a recommendation, we advise that one avoid making zoning changes to your fabric while data is being transferred, if possible. There may be some risk in job interruption, especially with serial data during the Registered State Change Notifications (RSCN's) that are produced as a result of the zone change. Some HBA's are more prone to an interruption than others.

IBM 2064 zSeries Servers

Description	Operating Systems	Additional Information
Ultrium 3584 UltraScalable Tape Library with Native FC Ultrium 2 drives only. (Feature Code 1476)	**IBM zSeries Servers Models z800 and z900** **SuSE Linux Enterprise Server 8** **FICON or FICON Express Channels** with FCP enablement firmware **Longware** • FC 2315 • FC 2319 **Shortware** • FC 2318 • FC 2320	Available **zSeries Support of Fibre Channel FCP Channels**

ROS nº 03/2005 - CN CPMI CORREIOS
Fls Nº 1201
3698
Doc.

IBM pSeries, RS/6000 and RS/6000 SP Servers

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame. **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 and 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module. **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives.	**AIX** • Version 4 • 4.3.3 • Version 5 • 5.1 • 5.2	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

11.032 Paula

IBM xSeries, Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 and 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives.	**Microsoft Windows NT** [4] • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server • Datacenter Server **Microsoft Windows 2003 Server** [5] • Standard Edition • Enterprise Edition • Datacenter Server • Web Edition	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Red Hat Advanced Server • 2.1 **SuSE Linux Enterprise Server (SLES)** • 7	Available Please review **RMSS Technical Support** Site.

[4] Windows NT 4.0 planed available on June 2003 for Ultrium 3582 Tape Library and Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2.
[5] Windows 2003 supports Ultrium 3582 Tape Library and Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2 only at this time.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1121
3698
Doc.

SUN microsystems Servers

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 drives. **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module	**Solaris** • 2.6 • 7 • 8 • 9	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
Ultrium 3584 UltraScalable Tape Library with Native FC Ultrium 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. [6] **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives. [7]	**Solaris** • 7 • 8 • 9	Available

[6] Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2- support available June 2003.
[7] Ultrium 3582 Tape Library with Native FC Ultrium 2- support available June 2003.

11.030 Folha

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 and 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. [8] **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives. [9]	**HP-UX** • 11.0 • 11i	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix. For specific details and restrictions please see the **readme** file.

[8] Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2- support available June 2003.
[9] Ultrium 3582 Tape Library with Native FC Ultrium 2 - support available June 2003.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 1122
3698
Doc

ECT
11.029
Paula

Manual 03

2109 Model C36 With Model M12
Installation and Service Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1123
3698
Doc.

ECT
11 028
Paulo

IBM TotalStorage SAN Cabinet

2109 Model C36 with Model M12 Installation and Service Guide

Read Before Using

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1121
3698
Doc.

GC26-7467-03

IBM TotalStorage SAN Cabinet

E.C.T. 11.027 Paula

IBM

2109 Model C36 with Model M12 Installation and Service Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 129
Doc. 3698

GC26-7467-03

11.026
Paula

Note:
Before using this information and the product it supports, read the general information in "Safety and environmental notices" on page xi, and "Notices" on page 123.

Fourth Edition (May 2003)

This edition replaces GC26-7467-02.

© Copyright International Business Machines Corporation 2002, 2003. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables ix

Safety and environmental notices xi
Safety notices xi
Safety inspection procedures xi
Inspecting the cabinet. xi
Inspecting the 2109 Model M12 xiv
Inspecting the bridge tool xviii
Environmental notices and statements xxi
Laser safety xxi
Battery notice xxii
Fire suppression systems. xxii
Product recycling. xxii
Product disposal xxii

About this document xxiii
Who should read this document xxiii
Additional information xxiii
2109 Model C36 with Model M12 library xxiii
Related documents xxiii
Web sites xxiv
Getting help xxiv
Getting software updates. xxiv
How to send your comments xxv

Chapter 1. Introduction 1
Overview 1
Software features 2
Port side of chassis 3
Blower assembly side of chassis 4
Monitoring and managing the 2109 Model M12 4

Chapter 2. Installing the 2109 Model C36 7
Step 1. Position the cabinet. 7
Step 2. Level the cabinet 8
Step 3. Attach the stabilizers 9
Step 4. Attach the cabinet to a concrete floor. 10
Step 5. Attach the cabinet to a concrete floor beneath a raised floor 12
Step 6. Attach the mounting plates 15
Step 7. Attach the front door 16
Step 8. Check the customer's ac power source 16
Step 9. Check the power distribution unit 17
External ac power cords 17
Step 10. Connect switch and device cables 18
Step 11. Power on the cabinet 18

Chapter 3. Starting and configuring the 2109 Model M12 19
Providing initial power to the chassis 19
Configuring the 2109 Model M12 19
Items needed 20
Configuration procedure 21

© Copyright IBM Corp. 2002, 2003

11.025 Paula

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1126
3698
Doc.

Chapter 4. Operating the 2109 Model M12 27
Turning on and off the 2109 Model M12. 27
Switch components 27
16-port cards 28
Control processor cards 28
Power supplies 30
ac power input connectors and ac power switches (circuit breaker). 30
Blower assemblies 30
WWN card and bezel 31
Cable management items 31
Interpreting LED activity 32
LEDs on the 16-port card 32
LEDs on the CP card 35
LEDs on the power supply 38
LEDs on the blower assembly 40
LEDs on the WWN card and bezel 41
Interpreting POST. 42
Maintaining the switch 43
Diagnostic tests 43
Field replaceable units 43
Environmental status and maintenance commands 44

Chapter 5. Installing modems 45
Setting up a remote modem system (optional) 46
Installing the modems on the 2109 Model M12 47
Verifying modem installation 48

Chapter 6. Installing and removing an additional 2109 Model M12 51
Installation considerations and safety guidelines. 51
Ordering the lift tool 52
2109 Model M12 standard shipment 53
Unpacking the 2109 Model M12 53
Installing the 2109 Model M12 in the cabinet 55
Time required 55
Tools required 55
Installing the brackets 55
Using the lift tool, the 24-inch load plate, and the bridge tool 60
Removing a 2109 Model M12 from the cabinet 65

Chapter 7. Servicing the 2109 Model C36 with Model M12. 69
Safety notices 69
Power-on procedure 69
Power-off procedure 70
Removing and replacing a 16-port card or filler panel. 70
Time required 70
Removing a 16-port card or filler panel 70
Replacing a 16-port card or filler panel 74
Guidelines for managing cables. 75
Removing and replacing a CP card or filler panel 75
Time required 76
Items required 76
Confirming a failed CP card 76
Recording critical switch information for a CP card. 77
Removing a CP card or filler panel 79
Replacing a CP card or filler panel 81
Verifying the operation of the new CP card 82

Replacing the CP card battery 86
Removing and replacing a power supply or filler panel 86
Time required 87
Removing a power supply or filler panel. 87
Replacing a power supply or filler panel. 89
Removing and replacing a blower assembly 89
Time required 90
Items required 90
Removing a blower assembly 90
Replacing a blower assembly 90
Removing and replacing the cable management tray 91
Time required 91
Items required 91
Removing a cable management tray 91
Replacing a cable management tray 92
Removing and replacing the WWN card. 93
Verifying if the WWN needs replacing 93
Data that is stored on the WWN card 94
Messages that might indicate WWN card failure. 94
Removing and replacing the PDU 94
Removing the PDU 95
Replacing the PDU 95
Removing and replacing the chassis door 95
Time required 95
Removing the chassis door 96
Replacing the chassis door 96
Removing and replacing the front or rear cabinet door 96
Removing the cabinet door 96
Replacing the cabinet door 97
Relocating the cabinet 97
Reference information for the fruinfoset command 97

Appendix A. Product specifications 99
2109 Model M12 components 99
Physical dimensions 99
2109 Model M12 and component weights 99
2109 Model C36 with Model M12 specifications 100
16-port card specifications 100
CP card specifications. 101
Fibre Channel port specifications. 102
Facility specifications 103
Power specifications 103
Environmental requirements 104
General specifications. 105
Regulatory specifications. 106
POST and Boot specifications. 107
Monitoring POST results 107
Boot 108

Appendix B. Parts information 109
Covers 109
Earthquake brace 110
Blank fillers 111
Stabilizers 112
Leveling feet 113
Power cords 113

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 127
3698
Doc.

Cabinet parts list 115
Power distribution unit (PDU) 116
2109 Model M12 parts list 117

Appendix C. Blank planning worksheets 119
Planning worksheet 119
Port configuration worksheet 120
Zone definition worksheet 121
Zone configuration worksheet 122

Notices 123
Trademarks. 124
Electronic emission statements 124
Federal Communications Commission (FCC) statement 124
Industry Canada compliance statement 124
Chinese Class A compliance statement 124
European Community compliance statement 125
Germany compliance statement 125
Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 126
Korean Government Ministry of Communication (MOC) statement 126
Taiwan class A compliance statement 126

Glossary 127

Index 141

Figures

1. Agency Certification label on the 2109 Model C36 . . . xii
2. Power supply cord caution label on the 2109 Model C36 . . . xii
3. High leakage current danger label on the 2109 Model C36 . . . xiii
4. Safety label on the 2109 Model M12 . . . xv
5. Linecord caution label . . . xv
6. Power supply cover caution label . . . xvi
7. Fusing caution label . . . xvi
8. Heavy load label . . . xvi
9. SFP label (front view) . . . xvii
10. SFP label (back view) . . . xvii
11. Bridge tool alignment label . . . xix
12. Tilt warning label . . . xx
13. Genie tool and load plate label . . . xx
14. Pinch point label . . . xxi
15. Port side of the 2109 Model M12 . . . 3
16. Blower assembly side of the 2109 Model M12 . . . 4
17. Caster wheel . . . 8
18. Adjusting the leveling feet . . . 9
19. Stabilizers . . . 9
20. Attaching the cabinet to a concrete floor . . . 10
21. Leveling the cabinet . . . 12
22. Attaching the cabinet to a raised floor . . . 13
23. Leveling the cabinet . . . 14
24. Attaching the mounting plate . . . 15
25. Attaching the front door . . . 16
26. 16-port card LEDs . . . 33
27. CP card LEDs . . . 36
28. Power supply LEDs . . . 38
29. Blower assembly LEDs . . . 40
30. LEDs on the WWN card and bezel . . . 42
31. 2109 Model M12 with two modems connected . . . 46
32. 2109 Model M12 on a pallet . . . 54
33. Removing the chassis door . . . 55
34. Placement of the shelf brackets and clip nuts on the cabinet rails . . . 56
35. Shelf brackets are installed on the rails (cabinet walls are not shown) . . . 57
36. Placing the clip nuts on the rear rails (service aisle side) . . . 58
37. Attaching the right and left flat upper mount brackets to the chassis . . . 59
38. Attaching the L-shaped upper mount brackets to the rails . . . 59
39. Rear view of cabinet and lift tool . . . 61
40. Locking the shelf into position . . . 62
41. Attaching the mount brackets to the cabinet rails . . . 63
42. Attaching the port side of the chassis to the cabinet rails . . . 64
43. Removing the chassis door . . . 65
44. 16-port card showing ejectors . . . 72
45. 16-port card filler panel . . . 73
46. CP card filler panel with one handle . . . 74
47. Alignment guides in the card slots . . . 75
48. CP card showing ejectors . . . 80
49. CP card filler panel with two ejectors . . . 81
50. Alignment guides in the card slots . . . 82
51. Location of the power supplies . . . 88
52. Power supply and filler panel . . . 89
53. Blower assembly side of the 2109 Model M12 shown with one blower assembly uninstalled . . . 91

© Copyright IBM Corp. 2002, 2003

11021 Paula

05/2005 - CN
CPMI - CORREIOS
Fls Nº 1128
Nº 3698
Doc.

54. Cable management tray 92
55. 2109 Model M12 with the cable management tray 93
56. Removing the cabinet door 96
57. Front view of the PDU 116
58. Top view of the PDU 117

Tables

1. Brocade and IBM product and model number matrix . . . xxiv
2. Configuration parameters . . . 21
3. 16-port card LED patterns . . . 33
4. CP card LED patterns . . . 37
5. Power supply LED patterns . . . 39
6. Blower assembly LED patterns . . . 40
7. Modem parameters for Windows 95, 98, 2000, ME, or NT, or TERM in a UNIX environment 47
8. Parameters and values . . . 77
9. Data that the WWN card stores . . . 94
10. Sample error messages . . . 94
11. Reference information for the fruinfoset command . . . 97
12. Physical dimensions of the 2109 Model M12 . . . 99
13. Component weights . . . 99
14. 2109 Model C36 with Model M12 specifications . . . 100
15. Memory specifications . . . 101
16. Battery specifications . . . 101
17. Pinouts with signal and description . . . 102
18. Modem serial port pinouts . . . 102
19. Power specifications . . . 104
20. Environmental requirements . . . 104
21. General specifications . . . 105
22. Regulatory specifications . . . 106
23. Items supplied with the 14U chassis mount kit . . . 115
24. Planning worksheet . . . 119
25. Port configuration worksheet . . . 120
26. Zone definition worksheet . . . 121
27. Zone configuration worksheet . . . 122

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1129
3698
Doc

Safety and environmental notices

This section contains information about:

- Safety notices that are used in this document
- Safety inspection procedures for this product
- Environmental guidelines for this product

Safety notices

This document contains the following safety notices:

A *Danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

A *Caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

An *Attention* notice indicates the possibility of damage to a program, device, system, or data.

Safety inspection procedures

This safety inspection procedure contains three parts:

- Inspecting the 2109 Model C36 cabinet
- Inspecting the 2109 Model M12 switch
- Inspecting the bridge tool, where applicable

This document uses the following terms:

- *Rack* refers to the metal framework of this unit.
- *Cabinet* refers to the rack, all the peripherals that are attached to the rack, and the 2109 Model M12 switch.

Inspecting the cabinet

Perform a safety inspection on the cabinet when any of the following conditions occur:

- The cabinet is inspected under a maintenance agreement.
- Service is requested and service has not recently been performed.
- An alteration-and-attachments review is performed.
- Changes were made to the equipment that might affect the safe operation of the equipment.
- External devices with an attached power cord are connected to the cabinet.

Be cautious of potential safety hazards that are not covered in the safety checks. If the inspection indicates an unacceptable safety condition, the condition must be corrected before you can service the machine.

Note: The owner of the system is responsible for correcting any unsafe condition.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1130
Doc. 3698

Cabinet safety label checks

Perform the following cabinet safety label checks:

1. Verify that the Agency Certification label shown in Figure 1 is installed on the 2109 Model C36.

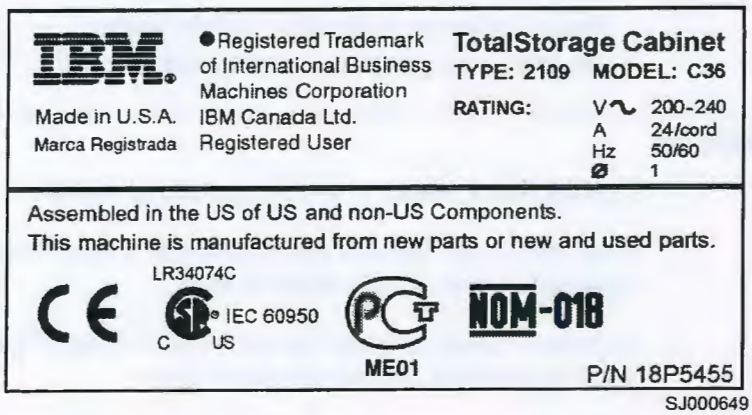


Figure 1. Agency Certification label on the 2109 Model C36

2. Verify that the power supply cord caution label shown in Figure 2 is installed on the 2109 Model C36.

   CAUTION:
   This unit has more than one power supply cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing.

Figure 2. Power supply cord caution label on the 2109 Model C36

3. Verify that the high leakage danger label shown in Figure 3 on page xiii is installed on the 2109 Model C36.

11.016 Paula

DANGER

HIGH LEAKAGE CURRENT. Earth connection essential before connection supply.

SJ000651

Figure 3. High leakage current danger label on the 2109 Model C36

External cabinet checks

Perform the following safety checks:

1. If the cabinet is bolted down, ensure that the cabinet is firmly secured to the floor. See Figure 20 on page 10.
2. If the cabinet is not bolted down, ensure that the stabilizers are firmly attached to both the bottom front and bottom rear of the rack. See Figure 19 on page 9.

   CAUTION:
   You must firmly attach the stabilizer to the bottom front and bottom rear of the cabinet to prevent the cabinet from turning over when the switches are pulled out of the cabinet.
3. Check the covers for sharp edges and for damage or alterations that expose the internal parts of the cabinet.
4. Check the covers for a proper fit to the cabinet. The covers should be in place and secure.
5. Open the rear door of the cabinet.
6. **CAUTION:**
   This unit might have more than one power supply cord. To completely remove power, you must disconnect all power supply cords.

   Perform the power-off procedure for the power distribution unit (PDU) that is installed in the cabinet. See "Power-off procedure" on page 70 for power-off procedures.
7. Check for alterations or attachments and obvious safety hazards such as broken wires, sharp edges, or broken insulation.

RQS nº 03/2005 - CN CRM/ CORREIOS
Fls Nº 1131
3698
Doc.

8. Check the internal cables for damage.
9. Check for dirt, water, and any other contamination within the cabinet.
10. Check the voltage label on the back of the system unit to ensure that it matches the voltage at the outlet.
11. Check the external power cable for damage.
12. Perform the following grounding checks:
    a. With the external power cord connected to the system unit, check for 0.1 ohm or less resistance between the ground lug on the external power cord plug and the rack.
    b. Using the appropriate probe, check for 0.1 ohm or less resistance between the rack and the grounding pin on each of the power outlets on each power distribution bus.
13. Check for the following conditions for each external device that has an attached power cord:
    - Damage to the power cord.
    - The correct grounded power cord.
    - With the external power cord connected to the device, check for 0.1 ohm or less resistance between the ground lug on the external power cord plug and the rack of the cabinet.
14. Close the rear door of the cabinet.
15. Perform the power-on procedure for the PDU that is installed in the cabinet. See "Power-on procedure" on page 69.

Inspecting the 2109 Model M12

Perform the following safety checks to identify unsafe conditions.

Removing ac power

Perform the following steps to remove the alternating current (ac) power:

1. Perform a controlled system shutdown.
2. Set the power switches on the 2109 Model M12 to the off position.
3. Disconnect the power cord from the power source.

External machine checks

Perform the following external machine checks:

1. Verify that all external covers are present and are not damaged.
2. Ensure that all latches and hinges are in correct operating condition.
3. Check the power cord for damage.
4. Check the external signal cable for damage.
5. Check the cover for sharp edges, damage, or alterations that expose the internal parts of the device.
6. Correct any problems that you find.

Internal machine checks

Perform the following internal machine checks:

1. Check for any non-IBM changes that might have been made to the machine. If any are present, obtain the "Non-IBM Alteration Attachment Survey" form, number R009, from the IBM branch office. Complete the form and return it to the branch office.
2. Check the condition of the inside of the machine for:
    - Metal or other contaminants

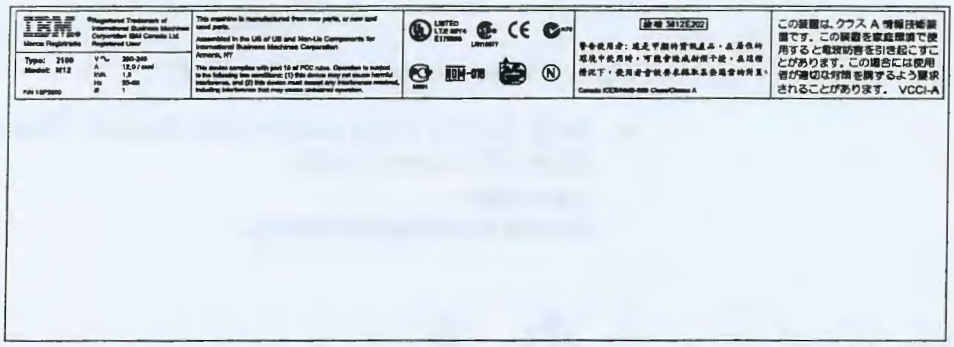
- Indications of water or other fluid
- Fire
- Smoke damage

3. Check for any obvious mechanical problems, such as loose components.
4. Check any exposed cables and connectors for wear, cracks, or pinching.

Safety label checks

Perform the following safety label checks:

1. Verify that the safety label shown in Figure 4 is installed on the 2109 Model M12.

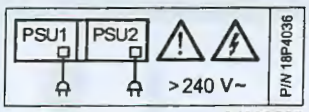


SJ000623

Figure 4. Safety label on the 2109 Model M12

2. Verify that the linecord caution label shown in Figure 5 is installed on the 2109 Model M12 power supply.

   CAUTION:
   This unit might have two linecords. To remove all power, disconnect both linecords.



SJ000620

Figure 5. Linecord caution label

3. Verify that the power supply cover caution label shown in Figure 6 is installed on the 2109 Model M12 power supply.

   CAUTION:
   Do not remove cover, do not service, no serviceable parts.

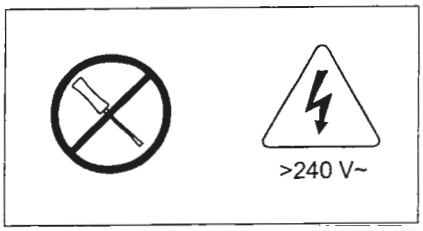


Figure 6. Power supply cover caution label

4. Verify that the fusing caution label shown in Figure 7 is installed on the 2109 Model M12 power supply.

   CAUTION:
   Double Pole/Neutral Fusing.

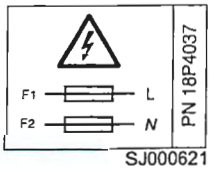


Figure 7. Fusing caution label

5. Verify that the heavy load label shown in Figure 8 is installed on the back of the 2109 Model M12.

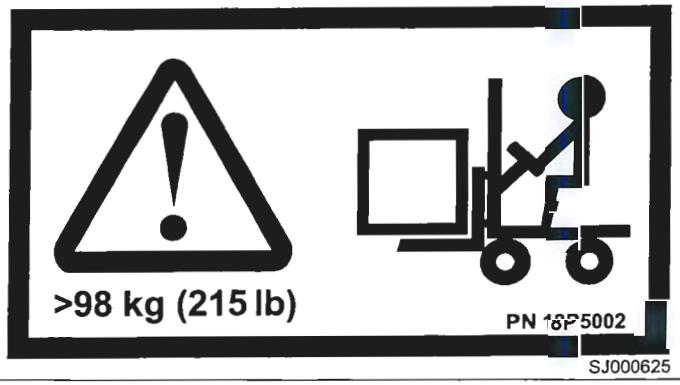
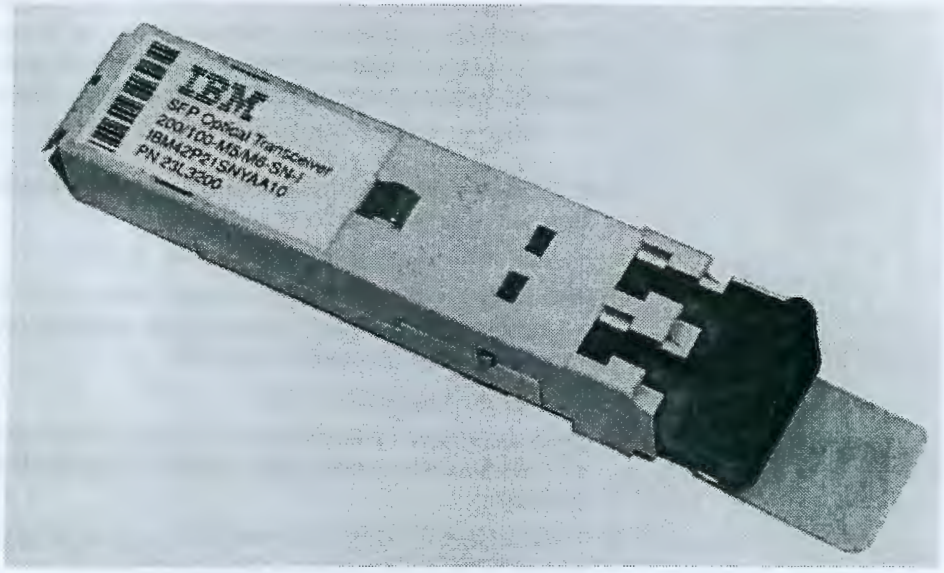


Figure 8. Heavy load label

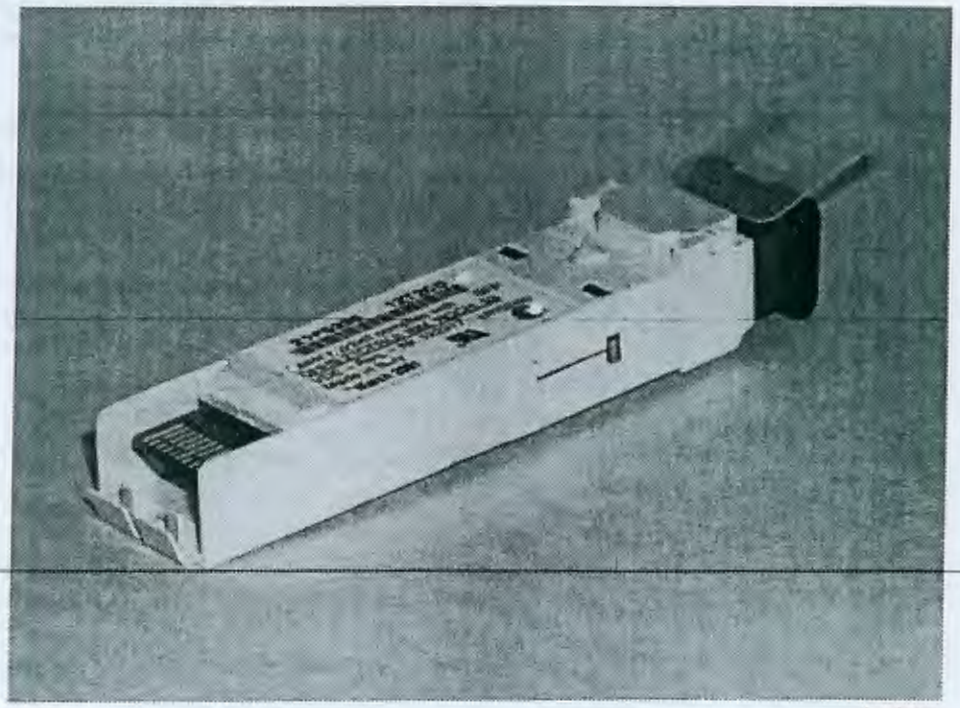
11.012
Paula

6. Verify that the SFP label shown in Figure 9 and Figure 10 is installed on the 2109 Model M12.



SJ000317

Figure 9. SFP label (front view)



SJ000314

Figure 10. SFP label (back view)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1118
3698
Doc.

Checking ac grounding

DANGER

An electrical outlet that is not correctly wired could place a hazardous voltage on the metal parts of the system or the products that attach to the system. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (1)

Check the voltage label on the bottom of the device to ensure that it matches the voltage at the power source.

1. Check the voltage level at the power source.
2. **Attention:** Always use an analog meter, never a digital meter, to perform the ground check of the customer's outlet. A digital meter can give the wrong reading if ground current is present.

   Check for proper grounding.
3. With the power cord connected to the 2109 Model M12, verify that there is 0.1 ohm or less resistance between the ground lug on the power cord plug and the rack.
4. If the 2109 Model M12 passes the ac grounding check (step 1 - step 3), connect the power cord to the power source.

Inspecting the bridge tool

Note: The bridge tool (PN 18P5855) is only shipped with a replacement 2109 Model M12 and is not part of the normal ship group. Inspect the bridge tool and ensure that the two adjustable supports are securely fastened and are rotated 90° from the base plate.

Perform the following safety label checks for the bridge tool:

1. Verify that the bridge tool alignment label shown in Figure 11 on page xix is installed on the load plate.

Figure 11. Bridge tool alignment label

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1131
3698
Doc.

2. Verify that the tilt warning label shown in Figure 12 is installed on the load plate.

SJ000750

Figure 12. Tilt warning label

3. Verify that the genie tool and load plate label shown in Figure 13 is installed on the load plate.

SJ000751

Figure 13. Genie tool and load plate label

4. Verify that the pinch point label shown in Figure 14 is installed on the load plate.

SJ000752

Figure 14. Pinch point label

Environmental notices and statements

This section describes the environmental notices and statements.

Laser safety

CAUTION:
In the United States use only GBIC units or Fibre-Optic products that comply with FDA radiation performance standards, 21 CFR Subchapter J. Internationally use only GBIC units or Fibre-Optic products that comply with IEC standard 825-1. Optical products that do not comply with these standards may produce light that is hazardous to the eyes.

SJ000327

This unit might contain a single-mode or a multimode transceiver Class 1 laser product. The transceiver complies with IEC 825-1 and FDA 21 CFR 1040.10 and 1040.11. The transceiver must be operated under the recommended operating conditions.

This equipment contains Class 1 laser products and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser-safety standard IEC 825-2.

Usage restrictions

Terminate the optical ports of the modules with an optical connector or a dust plug.

Battery notice

CAUTION:
A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery might present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations.

Fire suppression systems

A fire suppression system is the responsibility of the customer. The customer's own insurance underwriter, local fire marshal, or a local building inspector, or both, should be consulted in selecting a fire suppression system that provides the correct level of coverage and protection. IBM designs and manufactures equipment to internal and external standards that require certain environments for reliable operation. Because IBM does not test any equipment for compatibility with fire suppression systems, IBM does not make compatibility claims of any kind nor does IBM provide recommendations on fire suppression systems.

See "Environmental requirements" on page 104.

Product recycling

This unit contains recyclable materials. Recycle these materials where processing sites are available and according to local regulations. In some areas, IBM provides a product take-back program that ensures proper handling of the product. Contact your IBM representative for more information.

Product disposal

This unit might contain batteries. Remove and discard these batteries, or recycle them, according to local regulations.

11006
Paula

About this document

This document provides installation and maintenance information for the IBM® TotalStorage™ SAN Cabinet 2109 Model C36 with Model M12 switch.

This document uses the following terms:

- *Rack* refers to the metal framework of this unit.
- *Cabinet* refers to the rack, all the peripherals that are attached to the rack, and the 2109 Model M12 switch.

Who should read this document

This document is intended for the service support representative to install or repair the 2109 Model C36 with Model M12 switch.

Additional information

This section contains the following information:

- A list of the documents in the 2109 Model C36 with Model M12 library
- A list of the related documents
- The available Web sites
- Instructions on how to get help
- Instructions on how to get software updates
- Information about how to send your comments

2109 Model C36 with Model M12 library

The following documents contain information related to this product:

- *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*, GC26-7467 (this book)
- *IBM TotalStorage SAN Switch 2109 Model M12 User's Guide*, GC26-7468

Related documents

You can find Information related to the software that supports the 2109 Model M12 in the following documents:

- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Diagnostic and System Error Message Reference*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Reference*
- *Brocade Fabric Watch User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade MIB Reference*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Silkworm 12000 Core Migration User's Guide*

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 136
3698
Doc

- *Building and Scaling Brocade SAN Fabrics: Design and Best Practices Guide*

When you use any of the Brocade documents, you will notice that the model numbers reflect the original Brocade switches. Table 1 provides a product matrix for you to use to correlate the Brocade model numbers to the IBM product and model numbers.

Table 1. Brocade and IBM product and model number matrix

Brocade model number	IBM product and model number
Silkworm 2010	3534 Model 1RU
Silkworm 2400	2109 Model S08
Silkworm 2800	2109 Model S16
Silkworm 3200	3534 Model F08
Silkworm 3800	2109 Model F16
Silkworm 3900	2109 Model F32
Silkworm 12000	2109 Model M12

Web sites

For detailed information about models and firmware that the switch supports, see the following Web site:

www.ibm.com/storage/fcswitch/

For detailed information about Fibre Channel standards, see the Fibre Channel Association Web site at:

www.fibrechannel.com/

For a directory of worldwide contact information, including technical support, see the following Web site:

www.ibm.com/contact/

Getting help

Contact your switch supplier for technical support. This includes support of hardware, all product repairs, and ordering of spare components.

Be prepared to provide the following information to the support personnel:

- The switch serial number
- The switch worldwide name
- The topology configuration
- Any output from the **supportShow** Telnet command
- A detailed description of the problem
- Any troubleshooting steps that were already performed

Getting software updates

Contact your software vendor for software updates and maintenance releases.

For utility programs to facilitate loading firmware, sample Fabric Watch configurations, and management information base (MIB) files for switch management by simple network management protocol (SNMP), see the following Web site:

www.storage.ibm.com/ibmsan/products/sanfabric.htm

How to send your comments

Your feedback is important to help us provide the highest quality of information. If you have any comments about this document, you can submit them in one of the following ways:

- E-mail

  Submit your comments electronically to:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the document and, if applicable, the specific location of the text that you are commenting on, such as a page number or table number.

- Mail or fax

  Fill out the Readers' Comments form (RCF) at the back of this document and return it by mail or fax (1-800-426-6209) or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Dept. M86/Bldg. 050-3
  5600 Cottle Road
  San Jose, CA 95193-0001
  U.S.A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1698
Doc.

Chapter 1. Introduction

This chapter introduces the 2109 Model M12 switch (hereafter referred to as the 2109 Model M12) and contains the following information:

- Overview of the 2109 Model M12
- How to monitor and manage the 2109 Model M12

The IBM factory installs the 2109 Model M12 and ships it in the 2109 Model C36 cabinet.

Overview

The 2109 Model M12 is a high-performance core switch for large storage area networks (SANs), available in 16-port increments from 32 - 128 ports. It can operate as a single switch in a fabric or in a fabric that contains multiple switches.

High-availability features of the 2109 Model M12 include:

- Two redundant hot-swappable control processor (CP) cards with automatic failover
- Up to eight hot-swappable 16-port cards
- Four hot-swappable power supplies
- Three hot-swappable blower assemblies (two are required for adequate cooling)
- Two redundant ac inputs
- Non-disruptive upgrades for Fabric OS v4.1
- Worldwide name (WWN) card that is hot-swappable in Fabric OS v4.1

The 2109 Model M12 also includes the optional Advanced Security feature, which enables policy-based security mechanisms integrated with certain versions of the Fabric OS. The optional Advanced Security feature has the following capabilities:

- Centralized security management
- Fabric-wide security policies to control access
- Port and switch level access control
- Management access controls (Telnet, SNMP, HTTP, API)
- Encryption of management data such as passwords
- Strong and non-reputable authentication between switches

The Fibre Channel ports support link speeds of 1 Gbps and 2 Gbps (inbound and outbound). They also automatically negotiate to the highest common speed of all the devices that are connected to the port and are:

- Compatible with short wavelength (SWL) and long wavelength (LWL) small form factor pluggable (SFP) transceivers
- Universal and self-configuring
- Capable of individually becoming fabric loop ports (FL_ports), fabric ports (F_ports), or expansion ports (E_ports)

For the 2109 Model M12 specifications, see Appendix A, "Product specifications", on page 99.

© Copyright IBM Corp. 2002, 2003

ECT 11003 Paula
ROS nº 03/2005 - CN CPMI - CORREIOS Fls Nº 3698 Doc

Software features

Fabric OS version 4.1 supports the 2109 Model M12. Fabric OS includes all the basic switch and fabric support software as well as optionally licensed software that is enabled by using license keys. Fabric OS is made up of two major software components: firmware that initializes and manages the switch hardware, and diagnostics.

Optionally licensed and separately priced features include:

- Extended Fabrics (Feature code 7603)

  Provides up to 100 km (62.14 mi) of switched fabric connectivity at full bandwidth over long distances
- Remote Switch (Feature code 7602)

  Enables switches to interconnect over wide area network (WAN) using third-party gateway solutions that support Fibre Channel (FC) over Internet Protocol (IP), FC over asychronous transfer mode (ATM), and FC over SONET
- Advanced Security (Feature code 7623)

  Enables policy-based security mechanisms that are integrated within Fabric OS

Note: To activate these features, go to the following Web site:

www.ibm.com/storage/key/

The following licensed software provides a graphical user interface from a standard workstation:

- Fabric Manager 4.0 (Feature code 7203)

  Administers, configures, and maintains fabric switches and SANs with host-based software

The following licensed products are included with the 2109 Model M12:

- Performance Monitoring

  Comprehensive tool for monitoring the performance of network storage resources
- ISL Trunking

  Connects up to four ISLs between two switches through an expansion port (E_port) to merge logically into one link
- Fabric Watch

  Monitors mission-critical fabric parameters
- Advanced Zoning

  Segments a fabric into virtual private SANs
- Web Tools

  Administers, configures, and maintains fabric switches and SANs

---

See the following documents for more information about Fabric Watch, Fabric Manager, Web Tools, Secure Fabric OS, and high availability:

- *Brocade Advanced Zoning User's Guide*
- *Brocade Fabric Watch User's Guide*
- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Distributed Fabrics User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Advanced Web Tools User's Guide*

Port side of chassis

Figure 15 shows the port side of the 2109 Model M12, which provides access to the following components:

- The 16-port cards, which contains 16 Fibre Channel SFP ports
- Two CP cards, each with a modem serial port, a terminal serial port, and 10 Mbps or 100 Mbps Ethernet port
- Four power supplies that are hot-swappable and have built-in fans
- Two ac power connectors. Each ac power connector has an on or off ac power switch

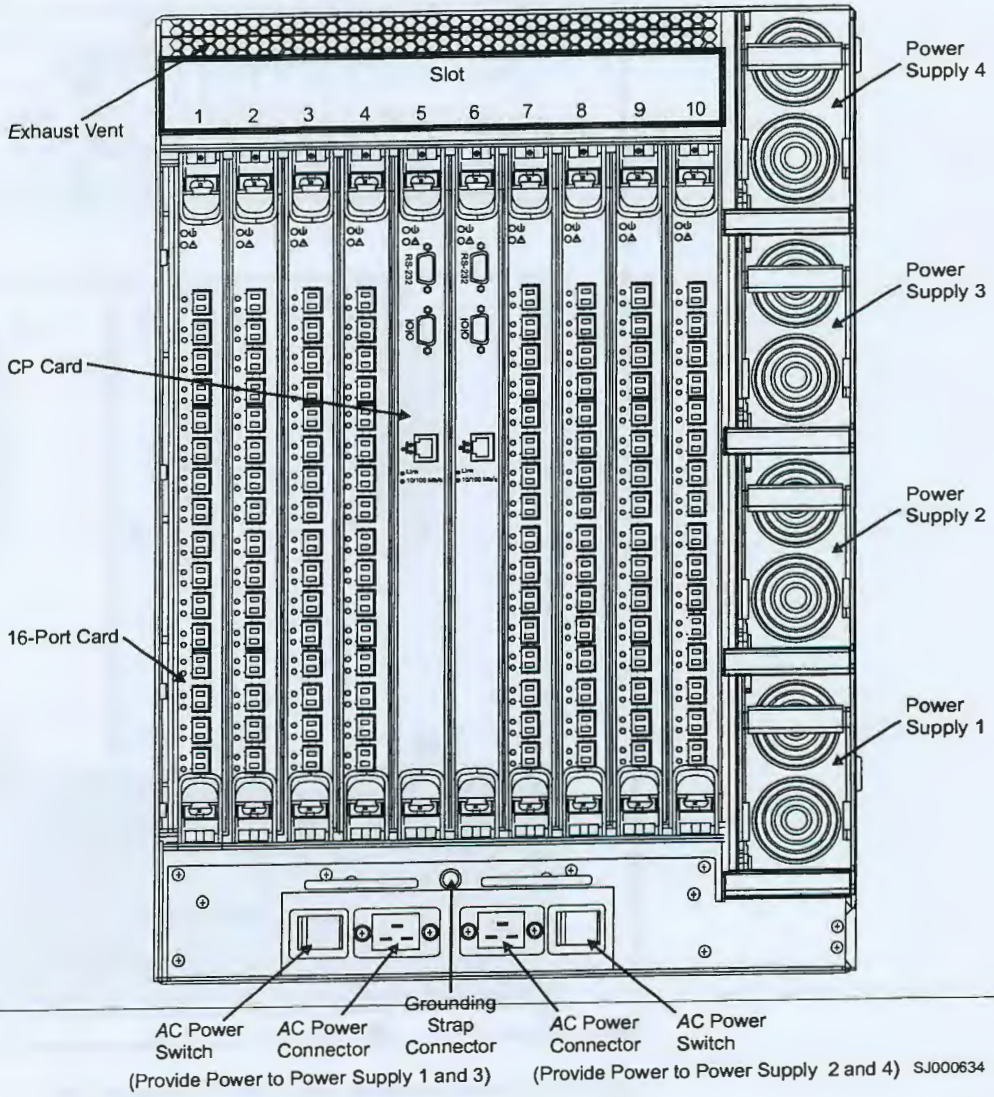


Figure 15. Port side of the 2109 Model M12

For information about how to operate the components of the 2109 Model M12, see Chapter 4, "Operating the 2109 Model M12", on page 27.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1101
3698
Doc.

Blower assembly side of chassis

Figure 16 shows the blower assembly side of the 2109 Model M12, which provides access to the following components:

- A WWN card and bezel. The WWN card and bezel provide light-emitting diodes (LEDs) for monitoring the switch from the blower assembly side and store WWN and IP address information, switch name, and serial number.
- Three blower assemblies. Each blower assembly is individually hot-swappable.

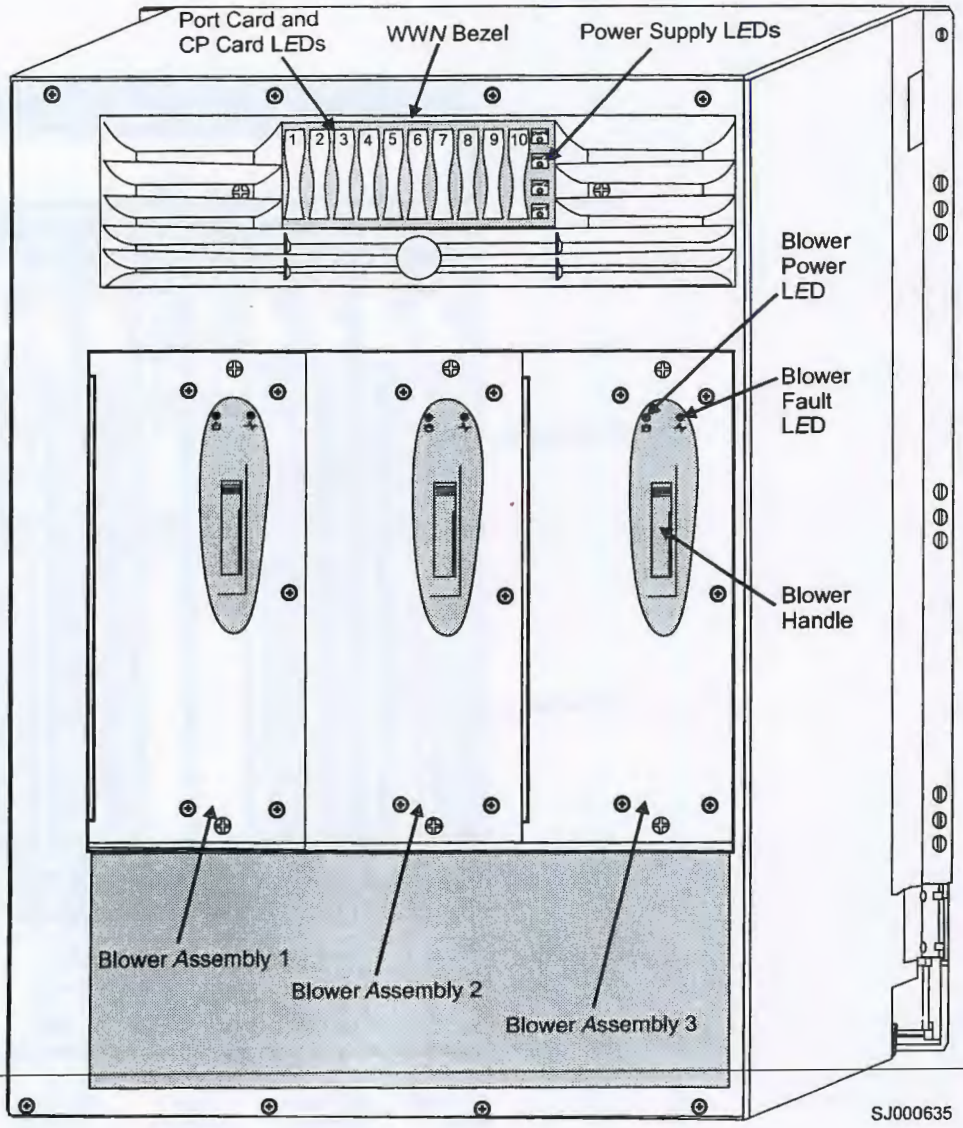


Figure 16. Blower assembly side of the 2109 Model M12

Monitoring and managing the 2109 Model M12

You can manage the 2109 Model M12 in-band by using Fibre Channel protocol or out-of-band by connecting to the Ethernet port. The management functions allow the administrator to monitor fabric topology, port status, physical status, and other information to aid in performance analysis and system debugging.

ECT
10 999
Paula

Note: The 2109 Model M12 automatically performs power-on self-test (POST) diagnostics each time it is turned on. Any errors are recorded in the error log. For more information about POST, see "Interpreting POST" on page 42.

The 2109 Model M12 is compatible with the following management interfaces:

- Command line interface through a Telnet connection
- Fabric Manager
- Web Tools
- SNMP applications
- Management server

You can manage these methods either in-band (Fibre Channel) or out-of-band (Ethernet).

For more information about these management interfaces, see the *Brocade Fabric Manager User's Guide* and the *Brocade Advanced Web Tools User's Guide*.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
3698
Doc.

10998 Paula

Chapter 2. Installing the 2109 Model C36

This section contains the procedures to install a 2109 Model C36 (hereafter referred to as the *cabinet*) and prepare it for use.

The following safety notices apply to the procedures in this chapter. Review this section carefully before you install the cabinet.

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

Before you install or remove signal cables, ensure that the power cables for the system unit and all attached devices are unplugged.

When you add or remove any additional devices to or from the system, ensure that the power cables for those devices are unplugged before you connect the signal cables. If possible, disconnect all power cables from the existing system before you add a device.

Use one hand, when possible, to connect or disconnect signal cables to prevent a possible shock from touching two surfaces with different electrical potentials.

During an electrical storm, do not connect cables for display stations, printers, telephones, or station protectors for communication lines.

CAUTION:
This product is equipped with a 3-wire power cable and grounded plug for the user's safety. Use this power cable in conjunction with a properly grounded electrical outlet to avoid electrical shock.

CAUTION:
This unit might have more than one power supply cord. To completely remove power, you must disconnect all power supply cords.

Step 1. Position the cabinet

Note: IBM must install the IBM 2109 Model C36.

Perform the following steps to position the cabinet:

1. Remove all packing and tape from the cabinet.
2. Position the cabinet according to the customer floor plan.
3. Lock each caster wheel by tightening the screw on the caster. See Figure 17 on page 8.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1141
Doc. 3698

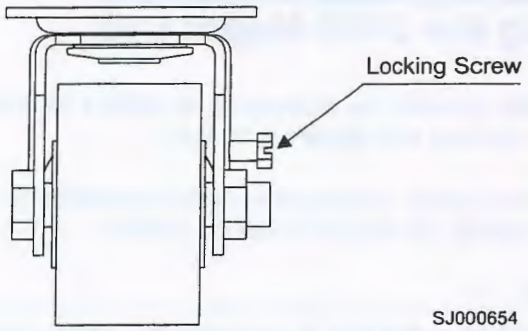


Figure 17. Caster wheel

Use the following conditions to determine the next step:

- If you are not attaching the cabinet to the floor, go to "Step 2. Level the cabinet".
- If you are bolting the cabinet to a concrete floor, go to "Step 4. Attach the cabinet to a concrete floor" on page 10.
- If you are bolting the cabinet to a concrete floor beneath a raised floor, go to "Step 5. Attach the cabinet to a concrete floor beneath a raised floor" on page 12.

Step 2. Level the cabinet

Perform the following steps to adjust the leveling feet:

1. Loosen the jam nut on each leveling foot by turning the nut counterclockwise, away from the bottom of the cabinet. See Figure 18 on page 9.
2. Rotate each leveling foot downward until it contacts the surface on which the cabinet is placed.
3. Adjust the leveling feet downward as needed until the cabinet is level. When the cabinet is level, tighten the jam nuts against the base by turning the nut clockwise, toward the bottom of the cabinet.

10996 Paula

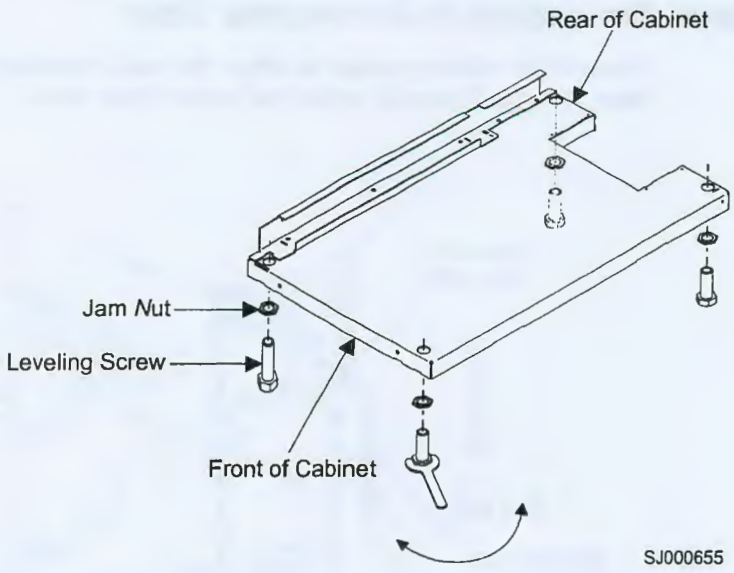


Figure 18. Adjusting the leveling feet

Step 3. Attach the stabilizers

CAUTION:
You must firmly attach the stabilizers to the bottom front and bottom rear of the cabinet to prevent the cabinet from turning over when the switches are pulled out of the cabinet.

1. Align the slots in the stabilizer with the mounting holes at the bottom front of the cabinet. See Figure 19.

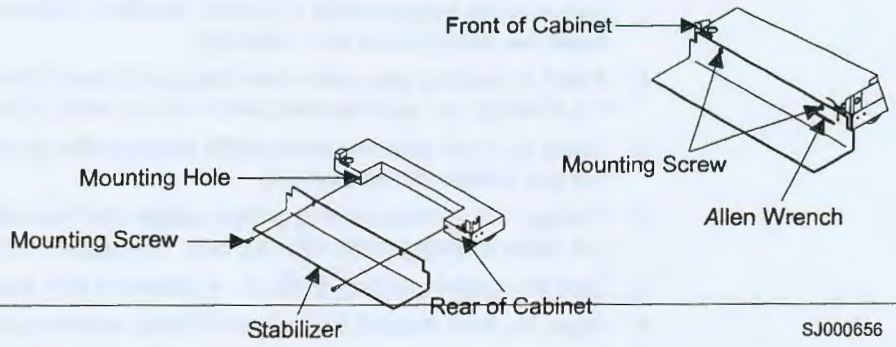


Figure 19. Stabilizers

2. Install the two mounting screws.
3. Ensure that the base of the stabilizer rests firmly on the floor. Use the allen wrench that is supplied with the cabinet to alternately tighten the mounting screws until they are tight.
4. Repeat step 1 through step 3 to install the stabilizer at the bottom rear of the cabinet.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1449
3698
Doc

Step 4. Attach the cabinet to a concrete floor

Perform the following steps to attach the rack-mounting plates directly to a concrete floor. Refer to Figure 20 while you perform the steps.

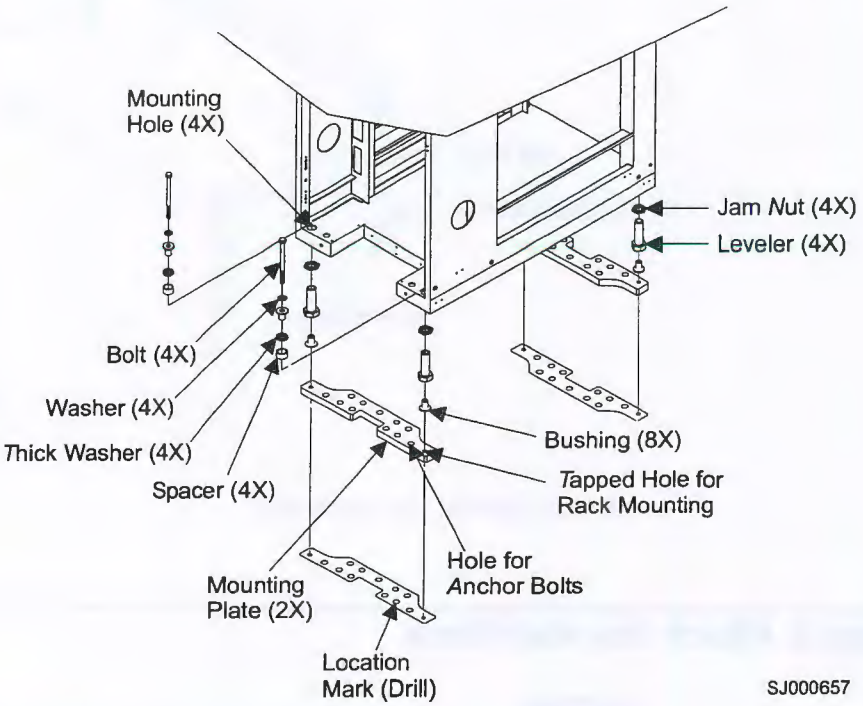


Figure 20. Attaching the cabinet to a concrete floor

1. Ensure that the cabinet is in the correct location.
2. In this cabinet, temporarily install the bushings to help position the rack-mounting plates.
3. Ensure that the bushing is in the leveling foot. Position the two rack-mounting plates in the approximate mounting location under the cabinet. If necessary, raise the leveling feet for clearance.
4. Place a bushing on a rack-mounting bolt. Insert the bolt and bushing through the leveling foot and bushing and out the bottom bushing.
5. Insert the four rack-mounting bolts through the leveling feet and bushings and out the bottom of the cabinet.
6. Position the rack-mounting plates under the four rack-mounting bolts. Center the rack-mounting bolts directly over the tapped holes.
7. Turn the rack-mounting bolts 3 - 4 rotations into the tapped holes.
8. Mark the floor around the edges of both rack-mounting plates.
9. Mark the rack-mounting plate bolt-down holes that are accessible through the opening in the rear of the cabinet.
10. Remove the rack-mounting bolts and bushings.
11. Remove the rack-mounting plates.
12. Loosen the locking screws on the casters. Move the cabinet so that the cabinet is clear of the locator marks for the rack-mounting plates.
13. Position the rack-mounting plates within the marked areas.

10 9924 Fls

14. Mark the floor at the center of each hole in the rack-mounting plates (including the tapped holes).
15. Remove the two rack-mounting plates from the marked locations.
16. At the marked location of the tapped rack-mounting bolt holes, drill four holes approximately 5 cm (2 in.). This allows clearance for the ends of the four rack-mounting bolts. The ends of the rack-mounting bolts protrude past the thickness of the mounting plate.

    Note: You must use a minimum of two anchor bolts for each rack-mounting plate to attach it to the concrete floor. Because some of the holes in the rack-mounting plates might align with the concrete reinforcement rods that are below the surface of the concrete, some of the rack-mounting plate holes might not be suitable.
17. For each rack-mounting plate, select at least two suitable holes. Select holes as close to the threaded holes as possible. Be sure that the holes you select at the rear of the cabinet are accessible. Drill the selected holes (two for each rack-mounting plate).
18. Position the front rack-mounting plate within the marked area.
19. Using anchor bolts, attach the front rack-mounting plate to the concrete floor.

    Note: Do not use the four plastic isolator bushings.
20. Position the cabinet over the front rack-mounting plate.
21. Position the rear rack-mounting plate within the marked area.
22. Using anchor bolts, attach the rear rack-mounting plate to the concrete floor.
23. Insert each of the rack-mounting bolts through a flat washer, a thick washer, and through a leveling foot.
24. Align the four rack-mounting bolts with the four tapped holes in the two rack-mounting plates and turn the bolts 3 - 4 rotations.
25. Tighten the locking screw on each caster.
26. Adjust the leveling screw downward, as needed, until the cabinet is level. See Figure 21 on page 12. When the cabinet is level, tighten the jam nuts against the base by turning the jam nut clockwise, toward the bottom of the cabinet. Torque the four bolts to 54 - 67 nm (40 - 50 ft-lbs).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 3698
Doc.

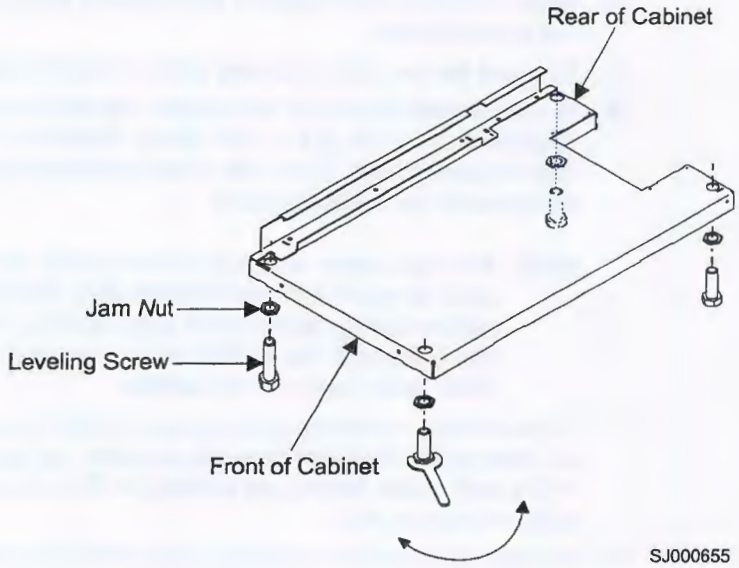


Figure 21. Leveling the cabinet

27. After you bolt down the cabinet, go to "Step 6. Attach the mounting plates" on page 15.

Step 5. Attach the cabinet to a concrete floor beneath a raised floor

Perform the following steps to attach the rack-mounting plates to the concrete floor beneath a raised floor.

Refer to Figure 22 on page 13 while you perform the steps.

ECT 10.992 Paula 251-53

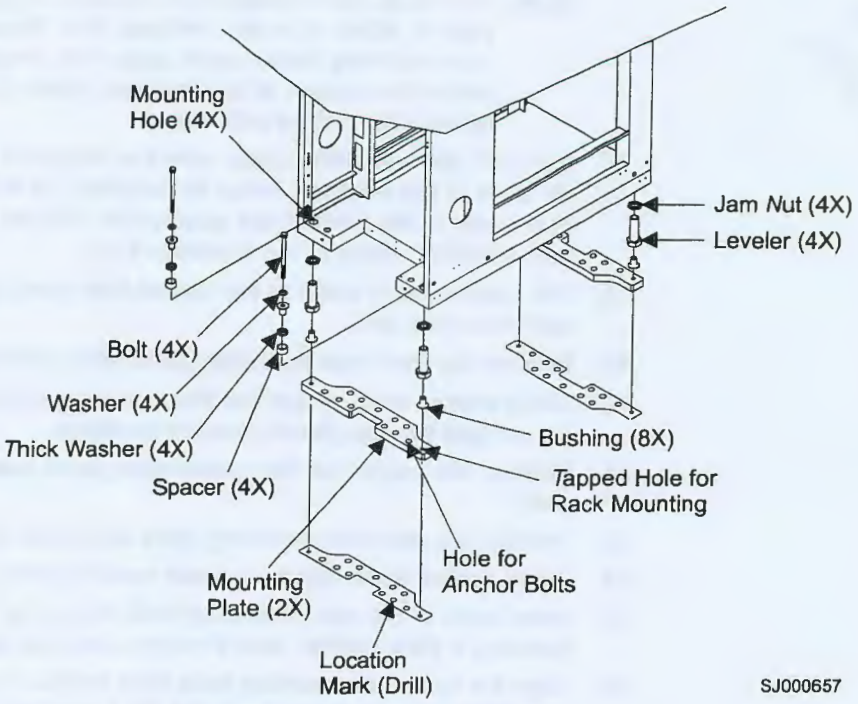


Figure 22. Attaching the cabinet to a raised floor

1. Ensure that the cabinet is in the correct location.
2. In this cabinet, temporarily install the bushings to help position the rack-mounting plates.
3. Ensure that the bushing is in the leveling foot. Position the two rack-mounting plates in the approximate mounting locations under the cabinet. If necessary, raise the leveling feet for clearance.
4. Place a bushing on a rack-mounting bolt. Insert the bolt and bushing through the leveling foot and bushing, and out of the bottom bushing.
5. Insert the four rack-mounting bolts through the leveling feet and bushings, and out the bottom of the cabinet.
6. Position the rack-mounting plates under the four rack-mounting bolts. Center the rack-mounting bolts directly over the tapped holes.
7. Turn the rack-mounting bolts 3 - 4 rotations into the tapped holes.
8. Mark the raised-floor panel around the edges of both rack-mounting plates.
9. Mark the rack-mounting plate bolt-down holes that are accessible through the opening in the rear of the cabinet.
10. Remove the rack-mounting bolts and bushings.
11. Remove the rack-mounting plates.
12. Loosen the locking screws on the casters. Move the cabinet so that it is clear of the locator marks for the rack-mounting plates.
13. Position the rack-mounting plates within the marked areas.
14. Mark the raised-floor panel at the center of each hole in the rack-mounting plates (including the tapped holes).
15. Remove the two rack-mounting plates from the marked locations.
16. Transfer the locations of the holes from the raised-floor panel to the concrete floor directly beneath. Mark the holes on the concrete floor.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 1141 Doc. 3698

Note: You must use a minimum of two anchor bolts for each rack-mounting plate to attach it to the concrete floor. Because some of the holes in the rack-mounting plates might align with concrete reinforcement rods below the surface of the concrete, some of the rack-mounting plate holes might not be suitable.

17. For each rack-mounting plate, select at least two suitable holes. Select holes as close to the threaded holes as possible. Be sure that the holes you select at the rear of the cabinet are accessible. Drill the selected holes (two for each rack-mounting plate) in the concrete floor.
18. Drill pass-through holes in the raised-floor panel at the location of the four rack-mounting bolts.
19. Position the front rack-mounting plate within the marked area.
20. Using anchor bolts, attach the front rack-mounting plate to the concrete floor. Do not use the four plastic isolator bushings.
21. Position the cabinet on the raised-floor panel over the front rack-mounting plate.
22. Position the rear rack-mounting plate within the marked area.
23. Using anchor bolts, attach the rear rack-mounting plate to the concrete floor.
24. Insert each of the rack-mounting bolts through a flat washer, a plastic isolator bushing, a thick washer, and through a leveling foot.
25. Align the four rack-mounting bolts with the four tapped holes in the two mounting plates and turn the bolts 3 - 4 rotations.
26. Tighten the locking screw on each caster.
27. Adjust the leveling feet downward, as needed, until the cabinet is level. See Figure 23. When the cabinet is level, tighten the jam nuts against the base by turning the jam nut clockwise (toward the bottom of the cabinet). Torque the four bolts to 54 - 67 nm (40 - 50 ft-lbs).

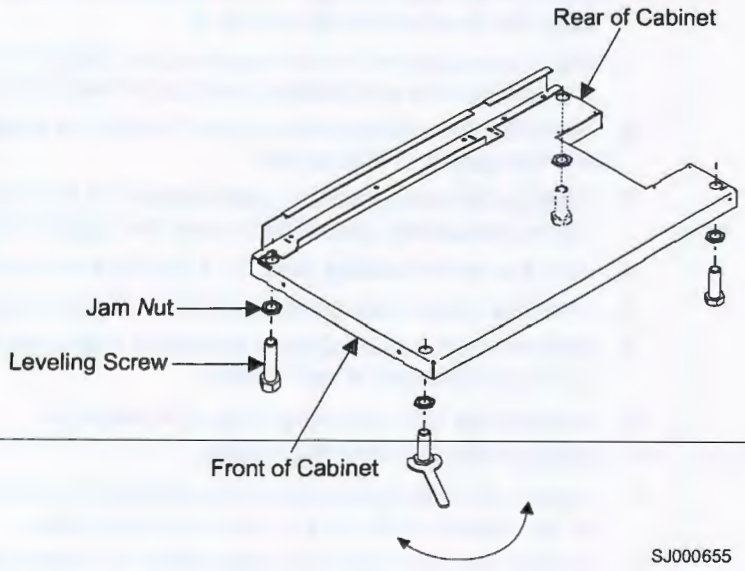


Figure 23. Leveling the cabinet

28. If the cabinet does not have a front door, install the top, left, and right trim panels.

29. After you bolt down the cabinet, go to "Step 7. Attach the front door" on page 16.

Step 6. Attach the mounting plates

Note: You attach the front and rear mounting plates through the same mounting holes that you use to mount the stabilizers. Therefore, you must bolt down the cabinet rather than use the stabilizers. Install the mounting plates *only* if you bolted the cabinet to the floor.

The mounting plates are part of the Earthquake Mounting Kit, feature code 6080.

Align the holes on the mounting plate with the holes on the front of the cabinet. Use the allen wrench that is supplied with the cabinet to install the mounting plate screws (stabilizer mounting screws). Repeat this procedure for the mounting plate on the rear of the cabinet. See Figure 24.

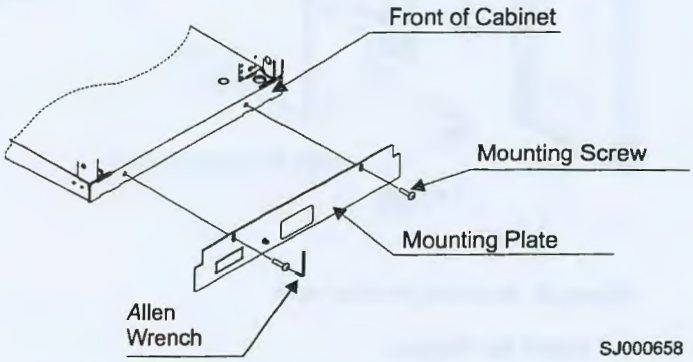


Figure 24. Attaching the mounting plate

Step 7. Attach the front door

If necessary, perform the following steps to attach the front door. Refer to Figure 25 while you perform the steps.

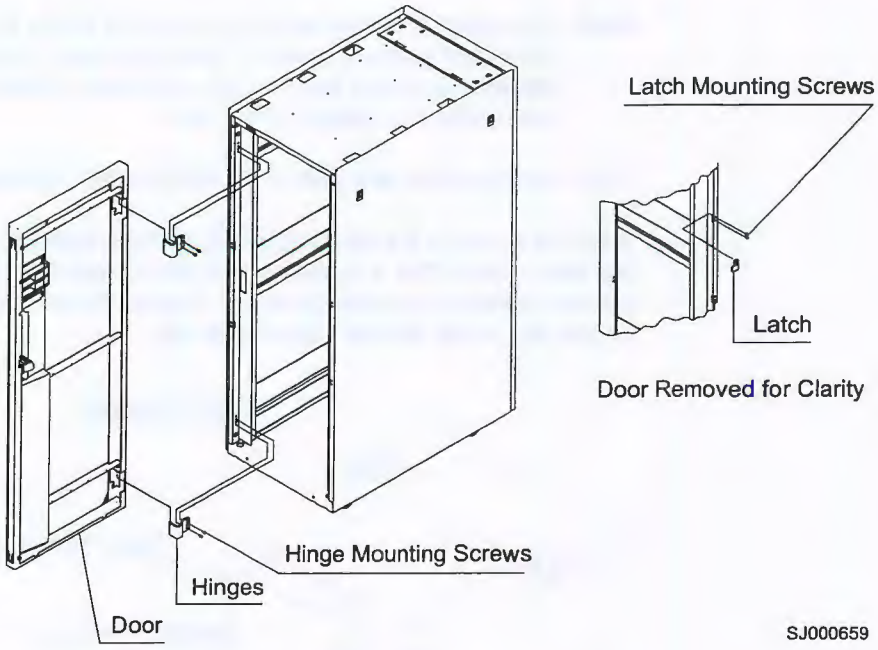


Figure 25. Attaching the front door

1. Install the hinges.
2. Install the latch.
3. Align the lower hinge pin on the front door with the hinge. Partially insert the pin into the hinge.
4. Align the upper hinge pin with the hinge. Lower the door into position.
5. Adjust the latch so that the door is latched securely.

Step 8. Check the customer's ac power source

Before you plug the power cord into the ac power source, perform the following checks on the customer's ac power source.

CAUTION:
Do not touch the receptacle or the receptacle face plate with anything other than your test probes before you meet the requirements in this step.

1. Have the customer turn off the branch circuit breaker for the ac power outlet into which the power cord will plug. Attach a "Do Not Operate" tag (S229-0237) to the circuit breaker switch.

   Note: All measurements are made with the receptacle face plate in the normal installed position.

2. Some receptacles are enclosed in metal housings. For this type of receptacle, perform the following steps:

10.988 Fls

a. Check for less than 1 volt from the receptacle case to any grounded metal structure, such as a raised-floor metal structure, water pipe, building steel, or similar structure.

b. Check for less than 1 volt from the receptacle ground pin to a grounded point in the building.

Note: If the receptacle case or face plate is painted, be sure that the probe tip penetrates the paint and makes good electrical contact with the metal.

c. Check the resistance from the ground pin of the receptacle to the receptacle case. Check the resistance from the ground pin to the building ground. The readings should be less than 0.1 ohm, which indicates the presence of a continuous grounding conductor.

3. If any of the three checks that you made in step 2 on page 16 are not correct, ask the customer to:
   - Remove the power from the branch circuit.
   - Make the wiring corrections.

   Recheck the receptacle.

   Note: Do not use a digital multimeter to measure grounding resistance in the following steps.
4. Check for infinite resistance between the ground pin of the receptacle and each of the phase pins. This check is for a wiring short to ground or a wiring reversal.
5. Check for infinite resistance between the phase pins. This check is for a wiring short.

   CAUTION:
   If the reading is other than infinity, do not proceed! Have the customer make the necessary wiring corrections before you continue. Do not turn on the branch circuit breaker until you satisfactorily complete all the previous steps.
6. Have the customer turn on the branch circuit breaker. Measure for the appropriate voltages between phases. If no voltage is present on the receptacle case or the ground pin, the receptacle is safe to touch.
7. With an appropriate meter, verify that the voltage at the ac outlet is correct.
8. Verify that the grounding impedance is correct by using the ECOS 1020, 1023, B7106, C7106, or an appropriately approved ground impedance tester.

Step 9. Check the power distribution unit

When the switch power cords are plugged into the power distribution unit (PDU) outlets, resistance should be less than 0.1 ohm between input ground and either switch or cabinet frames.

See "Power distribution unit (PDU)" on page 116 for an illustration and description of the PDU.

External ac power cords

To avoid electrical shock, the manufacturer provides a power cord with a grounded attachment plug. Use only properly grounded outlets.

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 1140
3698
Doc.

Power cords that are used in the United States and Canada are listed by Underwriter's Laboratories (UL) and are certified by the Canadian Standards Association (CSA). These power cords consist of the following parts:

- Electrical cables, type ST
- Attachment plugs that comply with National Electrical Manufacturers Association (NEMA) L6-30P
- Appliance couplers that comply with International Electrotechnical Commission (IEC) Standard 320, Sheets C13 and C14

Power cords that are used in other countries or regions consist of the following parts:

- Electrical cables, type HD21 or HD22
- Attachment plugs that the appropriate testing organization for the specific countries or regions where they are used has approved
- Appliance couplers that comply with International Electrotechnical Commission (IEC) Standard 320, Sheet C13 and C14

See "Power cords" on page 113 for information about the power cords that are available for the cabinet.

Step 10. Connect switch and device cables

The factory configures the cabinet and installs all of the switch cables.

If you need to install device cables, follow the installation instructions provided with the component that you are installing.

Step 11. Power on the cabinet

See "Power-on procedure" on page 69 for instructions on how to power on the cabinet.

ECT 10.986 Paula

Chapter 3. Starting and configuring the 2109 Model M12

You must configure the 2109 Model M12 appropriately in order for it to operate correctly within the network and fabric.

Note: The 2109 Model M12 only detects modems during power on or restart. If you connect a modem to an operating switch, you must restart the 2109 Model M12 in order for the switch to detect the modem.

This chapter describes how to start and configure the 2109 Model M12 and includes the following information:

- Providing initial power to the chassis
- Configuring, connecting, and accessing the 2109 Model M12

Providing initial power to the chassis

Perform the following steps to provide ac power to the chassis:

1. Connect the cabinet power distribution units (PDUs) to separate power sources of 200 - 240 V ac, 50 - 60 Hz.
2. Make sure that the internal power cords are connected to the separate PDUs and that the other ends are connected to the 2109 Model M12 circuit breakers.
3. Route the power cord so that it is not exposed to stress.
4. Flip both green ac power switches to "|". The ac power switches light up green when switched on, and power is being supplied.

The switch automatically performs a POST by default each time you power it on. A POST takes a minimum of 3 minutes. A POST is complete when light-emitting diode (LED) activity returns to a standard state. For information about LED light patterns, see "Interpreting LED activity" on page 32.

Attention: Do not connect the switch to the network until you configure the IP addresses.

Configuring the 2109 Model M12

The 2109 Model M12 can contain up to two logical switches, each with its own configuration:

- One logical switch for any 16-port cards in slots 1 - 4
- One logical switch for any 16-port cards in slots 7 - 10

The configuration information for both logical switches is stored in the WWN card and in the flash memory of the CP cards. The configuration is automatically mirrored to the standby CP card, so that the most current configuration remains available even if the active CP card fails. You can back up the configuration to a workstation by using the **configUpload** command. You can download the configuration to the active CP card by using the **configDownload** command. For information about commands and whether you can enter them through the active or standby CP card, see the *Brocade Fabric OS Reference*.

Note: You should routinely back up the configuration to ensure that the current configuration is available if needed.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN CPMI - CORREIOS Fls Nº 1147 Doc. 3698

You can modify the configuration only through a login session to the active CP card. The 2109 Model M12 supports up to two Telnet sessions with administrative privileges at the same time.

The same administrative login account applies to both logical switches. If the password is changed on switch 0, it automatically changes on switch 1.

The 2109 Model M12 configuration includes the following parameters:

- General system parameters

  You can modified these parameters with the **configure** command. For more information, see the *Brocade Fabric OS Reference*.
- WWNs for both logical switches

  You cannot modify the two WWNs. Both of them are preconfigured and are usually based on the chassis-serial number.
- Domain ID

  The default domain ID for both logical switches is 1. You can modify it by using the **configure** command.
- One domain ID for any of the 16-port cards in slots 1 - 4 and one for any of the 16-port cards in slots 7 - 10

  You can modify domain IDs with the **configure** command.
- Native IP addresses

  A native IP address, host name, subnetmask, and gateway address for both CP card slots. You can modify it by using the **ipAddrSet** command.
- Logical IP addresses

  A logical IP address and subnetmask for both logical switches. You can modify it by using the **ipAddrSet** command.

  Note: If you reset a logical IP address while the switch has active IP traffic, you can cause the IP traffic to be interrupted or stopped. IP traffic might include Web Tools, Fabric Watch, SNMP, and other applications.

Items needed

You will need the following items to configure and connect the 2109 Model M12:

- A 2109 Model M12 that is powered on and that is not connected to a network or fabric
- A workstation computer with a terminal emulator application, such as HyperTerminal
- The serial cable that is provided with the 2109 Model M12
- An Ethernet cable
- SFP transceivers and cables, as required
- Two IP addresses for the native IP addresses that are assigned to the CP slots, with the corresponding native host names, subnetmasks, and gateway addresses. The default native IP addresses and host names are as follows:
  - `10.77.77.75 CP0` (the CP card in slot 5 at the time of configuration)
  - `10.77.77.74 CP1` (the CP card in slot 6 at the time of configuration)
- Two IP addresses for the logical IP addresses of the switch, with the corresponding subnetmasks. These IP addresses correspond to "switch 0", which contains any 16-port cards in slots 1 - 4, and "switch 1", which contains any 16-port cards in slots 7 - 10. The default logical IP addresses are as follows:
  - `10.77.77.77 sw0`

10.984 Paula

  - `10.77.77.76 sw1`
- Two switch names, if the default switch names are not going to be used. Switch names can be up to 15 characters long. Switch names can include alphabetical, numerical, and underscore characters, and must begin with an alphabetical character. The default switch name for the logical switches is:
  - `sw0` for the switch that contains the 16-port cards in slots 1 - 4
  - `sw1` for the switch that contains the 16-port cards in slots 7 - 10

Configuration procedure

Note: The following procedure uses various Telnet commands. For information about these commands, see the *Brocade Fabric OS Reference*.

Perform the following steps to configure the 2109 Model M12:

1. Verify that the 2109 Model M12 is on. Verify that the POST is complete by verifying that all power LEDs on the 16-port cards and CP cards display a steady green light. For a description of the LED patterns, see "Interpreting LED activity" on page 32.
2. Login to the CP card that is installed in slot 5 by establishing a serial connection to a workstation that has a terminal emulator application, such as a HyperTerminal in a Microsoft® Windows® 95, Windows 2000, or Windows NT® environment, or TERM in a UNIX® environment.
   a. Disable any serial communication programs that are running on the workstation, such as synchronization programs for a PDA.
   b. Remove the shipping cap from the terminal serial port on the CP card in slot 5 and insert the serial cable. The terminal serial port is the second serial port from the top of the CP card.
   c. Connect the other end of the serial cable to a serial port on the workstation. If necessary, you can remove the adapter on the serial cable to allow for an RJ-45 serial connection.
   d. Open the terminal emulator application and configure as follows:
      - For a Windows 95, 98, 2000, or NT environment, use the configuration parameters shown in Table 2.

Table 2. Configuration parameters

Parameter	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

      - In a UNIX environment, type the following command:

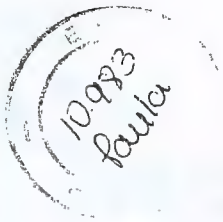
        ```
        tip /dev/ttyb -9600
        ```

   e. When the terminal emulator application stops reporting information, press Enter. The following login prompt displays:

```
CP Console Login:
```

   f. Type the logon information.

RQS nº 03/2005 - CN CPMI - CORREIOS
Fls. Nº 1145
Doc. 3698



The default administrative logon is `admin`, and the default password is `password`.

g. At the prompt, type `0` to log in to switch 0.

```
Enter switch number to login <0 or 1>:0
```

Note: At the initial login, the user is prompted to type a new admin password and a new user password. The same administrative account applies to both logical switches. If the password is changed on switch 0, it automatically changes on switch 1.

h. Change the passwords if desired. Passwords must be a total of 8 - 40 characters long and should include a combination of numbers, uppercase, and lowercase letters. To skip changing the password, press CTRL+C.

3. Type the following command to determine which CP card is active:

   `haShow`

   Information about the card displays. For example:

```
switch:admin> haShow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA Enabled, Heartbeat Up, HA State not in sync
```

4. Configure the IP addresses for both CP cards.

   You can make configuration changes only through a login session with the active CP card. However, you can assign IP addresses to either CP card from a login session with the active CP card.

   a. If the CP card in slot 5 is not the active CP card, disconnect the serial cable from the CP card, connect it to the CP card in slot 6, and login as `admin`.

   b. At the prompt, type `ipAddrSet 2` for the CP card in slot 5, or type `ipAddrSet 3` for the active CP card in slot 6.

   c. Type the requested information at the prompts, as the following example shows. The default information for the CP card in slot 5 is shown.

```
Ethernet IP Address [10.77.77.75]:
Ethernet Subnetmask [255.0.0.0]:
Host Name [CP0]:
Gateway Address [0.0.0.0]:
```

   The host name is the native name that is assigned to the CP card. You must use the same gateway address for both CP cards. These gateway addresses are referenced for the logical IP addresses.

   The native IP address of the active CP card is updated immediately. The native IP address of the standby CP card is updated at the next restart.

   d. Repeat step 4a - step 4c for the other CP card.

5. Configure the two logical IP addresses.

   Note: Resetting a logical IP address while the switch has active IP traffic can cause the IP traffic to be interrupted or stopped. IP traffic might include Web Tools, Fabric Watch, SNMP, and other applications.

If you change the IP address, you can cause a domain address format registered state change notification (RSCN) to be issued.

a. To configure the first logical IP address, type the following command at the prompt:

```
ipAddrSet 0
```

b. Type the requested information for this IP address at the prompt:

```
Ethernet IP Address [10.77.77.77]:
Ethernet Subnetmask [0.0.0.0]:
Fibre Channel IP Address [none]:
Fibre Channel Subnet Mask [none]:
```

The logical IP address is updated immediately.

c. To configure the second logical IP address, type the following command at the prompt:

```
ipAddrSet 1
```

d. Type the requested information for this IP address at the prompts.

e. At the prompt, type the following command to restart the CP card:

```
reboot
```

Note: You can use the terminal serial port to monitor error messages through a serial connection. Do not use the terminal serial port as a command line interface during normal operations because it only modifies one switch at a time (switch 0 by default).

f. If this port is not used continuously, remove the serial cable. Replace the shipping cap to protect the port from dust.

6. Optional: Connect the active CP card by Ethernet cable to the local area network (LAN).
   a. Remove the shipping plug from the Ethernet port on the active CP card.
   b. Insert one end of an Ethernet cable into the Ethernet port.
   c. Connect the other end to an Ethernet 10/100BASE-T LAN.

   You can now access the switch remotely by using any of the available management tools, such as Telnet or Web Tools. Be sure that the switch is not modified from other connections during the rest of this procedure.
7. Optional: Login to either of the logical switches by Telnet, using the administrative logon. The default administrative logon name is `admin`, and the default password is `password`.

   You can now access the switch remotely using Telnet or Web Tools. Be sure that the switch is not being modified from any other connections during the remaining steps. The 2109 Model M12 supports up to two Telnet sessions with administrative privileges at the same time. You can accomplish the remaining steps in this procedure with either a serial connection or a Telnet session.
8. Optional: Customize the switch names for the logical switches, if desired. If possible, use the default switch names.

   Note: Changing the name of the switch causes a domain address format RSCN to be issued.

   a. Type `switchName`, with the new switch name enclosed in double quotation marks. In the following example, `"sw10"` is the new switch name.

      ```
      switchName "sw10"
      ```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc. 3698

10981 Paula

b. Record the new switch name for future reference.

c. To customize the switch name for the other logical switch, perform the following steps:

1) Log out from the CP session.

2) Connect the serial cable to the other CP card.

3) Log in as admin.

4) Repeat step 8a on page 23 and step 8b for the other logical switch.

9. Optional: Modify the domain IDs, if desired.

Type `fabricShow` to see a list of the current domain IDs.

Note: The default domain ID for both switches is 1. To prevent a domain ID conflict, make the domain IDs unique before you connect the switches to the fabric.

a. Type the following command to disable the switch:

```
switchDisable
```

b. Type the following command:

```
configure
```

c. Type `y` at the `Fabric parameters` prompt:

```
Fabric parameters (yes, y, no, n): [no] y
```

d. Type a unique domain ID at the `Domain` prompt:

```
Domain: (1..239) [1] 3
```

e. Complete the remaining prompts or press CTRL+D to accept the other settings and exit.

f. Type the following command to re-enable the switch:

```
switchEnable
```

10. Optional: Specify any custom status policies.

a. To access the status policy, type the following command at the prompt:

```
switchStatusPolicySet
```

b. Complete the prompts to specify the status policies. To completely deactivate the alarm for a particular condition, type `0` at the prompt for that condition.

11. Add SFPs and cables to the Fibre Channel ports, as required.

Note: The ports are color-coded to indicate which ones can be used in the same trunking groups. Four ports that are marked with black solid ovals alternate with four ports that are marked with oval outlines. The ports and cables that are used in trunking groups must meet specific requirements. For a list of these requirements, see the *IBM TotalStorage SAN Switch 2109 Model M12 User's Guide* and the *Brocade ISL Trunking User's Guide.*

a. Position one of the SFPs so that the key is oriented correctly to the port. Insert the SFP into the port until it is firmly seated. Ensure that the latching mechanism clicks.

Note: SFPs are keyed so that you can only insert them with the correct orientation. If an SFP does not slide in easily, ensure that it is

10980 Paula

correctly oriented. For instructions that are specific to the SFP model, see the documentation of the SFP manufacturer.

b. Position a cable so that the key (the ridge on one side of the cable connector) aligns with the slot in the SFP. Insert the cable into the SFP until the latching mechanism clicks.

Note: Cables are keyed so that you can only insert them with the correct orientation. If a cable does not slide in easily, ensure that it is correctly oriented.

c. Repeat step 11a on page 24 and step 11b for the remaining ports.

d. Organize the cables as required.

12. Check the 2109 Model M12 for switch and port status. Type the following command at the Telnet prompt:

    `switchShow`

    This command provides detailed information about the switch.

13. Check the fabric for ISLs, switch names, or other status. Type the following command at the Telnet prompt:

    `fabricShow`

    This command provides general information about the fabric.

14. After all zoning configurations and other changes are complete, back up the configuration. Type the following command at the Telnet prompt:

    `configUpload`

    This command uploads the switch configuration to the server, so that it is available for downloading to a replacement switch if necessary.

    Note: You should routinely back up the configuration.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 117
3698
Doc.

10979
Paula

Chapter 4. Operating the 2109 Model M12

This chapter describes how to operate the 2109 Model M12 and includes the following information:

- Turning on and off the 2109 Model M12
- Interpreting LED activity
- Interpreting POST
- Maintaining the switch

Note: Throughout this chapter, the term *switch* refers to the 2109 Model M12.

Turning on and off the 2109 Model M12

Note: To provide power to the switch for the first time, see "Power-on procedure" on page 69.

To turn on the 2109 Model M12, verify that both power cords connect to the ac power connectors on the front of the chassis. Flip both green ac power switches to "|". The green ac power switches illuminate when they are on.

To turn off the 2109 Model M12, flip both ac power switches to "O". To remove all sources of power from the switch, disconnect both power cords from the power source.

Note: Removing all power from the switch triggers a system reset. When you restore the power, all devices return to the initial state, and the switch runs a POST.

Attention: After you power on the 2109 Model M12, run it for a minimum of 10 minutes before you power off again.

Switch components

The 2109 Model M12 includes the following components:

- 16-port cards
- CP cards
- Power supplies
- ac power input connection
- ac power switches
- Blower assemblies
- WWN card and bezel
- Cable management tray

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1101
Doc: 3698

16-port cards

Attention: Wear an electrostatic discharge (ESD) grounding strap when you work with a 16-port card to prevent damage to the electrical components.

To ensure correct cooling of the chassis and protection from dust, install a filler panel in any slots that do not contain a 16-port card.

Disassembling any part of a 16-port card voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the 16-port card.

Each 16-port card provides 16 auto-sensing Fibre Channel ports that are capable of auto-sensing data transmission speeds of 1 Gbps and 2 Gbps.

You can install 16-port cards in any combination of slots 1 - 4 (switch 0) and 7 - 10 (switch 1), with one exception. If there are one or more 16-port cards in slots 7 - 10, there must be at least one 16-port card in slots 1 - 4.

The ports on each of the 16-port cards are color-coded. The color code indicates which ports to use in the same ISL Trunking group. Four ports that are marked with black solid ovals alternate with four ports that are marked with oval outlines.

Note: ISL Trunking is a Fabric OS feature. ISL Trunking enables distribution of traffic over the combined bandwidth of up to four ISLs between two directly adjacent switches, while preserving in-order delivery. For more information about ISL Trunking, see the *Brocade ISL Trunking User's Guide*.

The 2109 Model M12 can continue to operate while you replace a 16-port card, but you must disconnect any devices that are connected to the 16-port card. To ensure correct air circulation inside the switch and protection from dust, you can order filler panels for any empty slots.

Perform the following steps to determine the status of a 16-port card:

1. Check the LEDs on the 16-port card. See Table 3 on page 33 for information about how to interpret the LEDs.
2. Check the 16-port card status by using the **slotShow** command. For additional information about this command, see the *Brocade Fabric OS Reference*.

Control processor cards

Attention: Wear an ESD grounding strap when you work with a CP card to prevent damage to the electrical components.

To ensure correct cooling of the chassis and protection from dust, install a filler panel in any slots that do not contain a CP card.

Disassembling any part of a CP card voids the part warranty and regulatory certifications. No user-serviceable parts are inside the CP card.

High availability is provided through redundant CP cards: An active CP card and a standby CP card. The active CP card is the one that is actively controlling the 2109 Model M12. If the active CP card failed or is uninstalled, the standby CP card

automatically becomes the new active CP card. Failover occurs as soon as the active CP card is detected to be faulty or uninstalled.

Information about both CP cards, including which card is active, is available by using the **haShow** command. For information about commands and whether you can enter them through the active or standby CP card, see the *Brocade Fabric OS Reference*.

Each CP card provides the following ports:

- Modem serial port

  The modem serial port has an RS-232 connector that is wired as a data terminal equipment (DTE) device. It is designed to connect to a distributed computing environment (DCE) device, such as a modem.
- Terminal serial port (also known as a console port)

  The terminal serial port has an RS-232 signal subset connector that you can use to connect to a PC serial port or dumb terminal.
- Ethernet port

  The Ethernet port has an RJ-45 connector and is capable of speeds of 10 Mbps or 100 Mbps.

You can connect a separate modem to each modem serial port, and then connect to the same or separate telephone lines for redundancy.

Note: The 2109 Model M12 only detects modems during power on or restart. If a modem is connected to an operating switch, you must restart the 2109 Model M12 in order to detect the modem.

The 2109 Model M12 can continue to operate while a CP card is being replaced. To ensure correct air circulation inside the switch and protection from dust, you can order filler panels for any empty slots.

The active CP card controls the following services:

- System initialization
- High availability and switch drivers
- Name server
- SNMP
- Fabric OS
- Extended Fabrics
- Fabric Watch
- Remote Switch
- Web Tools
- Zoning

Perform the following steps to determine the status of a CP card:

1. Check the LEDs on the CP card. See Table 4 on page 37 for information about how to interpret the LEDs.
2. Check the CP card status by using the **slotShow** and **haShow** commands.

   For additional information about these commands, see the *Brocade Fabric OS Reference*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1152
Doc. 3698

Power supplies

The 2109 Model M12 uses four power supplies. A minimum of two power supplies is required to power a completely loaded chassis.

The 2109 Model M12 can continue operating while a power supply is being replaced if at least one power supply continues operating for every four 16-port cards that are installed. You must have a minimum of two power supplies.

Attention: To protect against ac failure, you must have a minimum of one power supply in slot 1 or slot 3 and one in slot 2 or slot 4. If you install only two power supplies and you install both of them in slots that correspond to the same power cable, unplugging a single power cable will power down the entire chassis.

Attention: Disassembling any part of the power supply voids the part warranty and regulatory certifications.

Attention: Before you replace a power supply, determine whether adequate power will be available to keep the chassis operating throughout the replacement. If not, shut down both switches before you continue. If adequate power is abruptly lost, such as through removal of a power supply, the entire switch is powered down. The power off order that is designated by the **powerOffListSet** command is not followed.

CAUTION:
No user-serviceable parts are inside the power supply.

Perform the following steps to determine the status of a power supply:

1. Check the LEDs on the power supply. See Table 5 on page 39 for information about how to interpret the LEDs.
2. Check the power supply status by using the **psShow** command. The power supply status displays OK, absent, or faulty. For additional information about the **psShow** command, see the *Brocade Fabric OS Reference*.

ac power input connectors and ac power switches (circuit breaker)

The 2109 Model M12 has two ac power input connectors, each with a green ac power switch (circuit breaker). The left power input connector provides power to the power supplies in slot 1 and slot 3. The right power input connector provides power to the power supplies in slot 2 and slot 4. The power input connectors and their associated power supplies are color-coded.

Attention: Unplugging a single power cable can power down the entire switch, depending on which power supply slots contain power supplies.

Two detachable power cords are provided with the cabinet and are customized for the country or region in which it is installed.

The ac power switches light up green when they are on.

Blower assemblies

Three blower assemblies that are located in the back of the chassis cool the 2109 Model M12. The air enters through the vents in the blower assembly side of the chassis. The air exits from the top vent on the port side of the chassis. Each switch requires a minimum airflow of 350 cubic feet per minute.

10975 Fls.

The blower assemblies are hot-swappable if two blower assemblies remain operating. If you remove more than one blower assembly at the same time, turn off the 2109 Model M12 to prevent overheating.

Note: The 2109 Model M12 requires a minimum of two functioning blower assemblies during operation. To ensure continuous adequate cooling, maintain three operating blower assemblies at all times except for the brief period when replacing a blower assembly. The 16-port cards automatically shut down if the temperature range is exceeded.

Attention: Disassembling any part of the blower assembly voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the blower assembly.

Perform the following steps to determine the status of a blower assembly:

1. Check the LEDs on the blower assembly.
2. Check the blower assembly status by using the **fanShow** command. The status for each blower assembly displays OK, absent, or faulty. For additional information about the **fanShow** command, see the*Brocade Fabric OS Reference*.

WWN card and bezel

The WWN card and bezel are located at the top of the chassis on the blower assembly side. The WWN card has LEDs that you use to monitor the 2109 Model M12. The WWN card also stores the following information:

- The chassis serial number (used when installing software licenses)
- The two native IP addresses that are assigned to the CP card slots
- The logical switch names, IP addresses, and WWNs for the two logical switches

The bezel protects the card and identifies each of the LEDs on the WWN card. Together, the WWN card and bezel assembly provides a consolidated view of the LEDs for the two CP cards, eight 16-port cards, and four power supplies. If a slot contains a filler panel, the corresponding LEDs on the WWN card are not illuminated.

Note: There are two types of WWN cards. One type is attached to the chassis by screws and the other type is held on by the pressure of the bezel against a pad on the card face.

Attention: Although the information that is stored in the WWN card is also stored in the flash memory of the CP cards, do not restart the switch while the WWN card is uninstalled. Restarting the switch can cause the switch to start incorrectly.

Attention: Wear an ESD grounding strap when you work with the WWN card to prevent damage to the electrical components.

Cable management items

Two items are provided to assist with cable management:

- Cable management tray

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1153
Doc. 3698

The cable management tray is attached to the bottom of the chassis. You can use it to route the power cables and other cables down below the chassis or out the sides of the chassis.

- Cable guides

  A set of 16 cable guides is provided with the cabinet. You can use the guides to organize the port cables into logical groups, such as according to port quads (sets of four neighboring ports). The cable guides are free-floating and do not attach to the chassis. The cable guides keep the cables evenly spaced and hold them away from the 16-port cards. This makes card replacement easier and prevents the cables from bending to less than the minimum bend radius.

  Attention: Do not route the cables in front of the air exhaust vent, which is located at the top of the port side of the chassis.

  The minimum bend radius for a 50-micron cable is 3.05 cm (2 in.) under full tensile load, and 3.048 cm (1.2 in.) with no tensile load.

  Do not use tie wraps for optical cables because they are easily overtightened.

Interpreting LED activity

You can determine system activity and status by monitoring the activity of the LEDs on the switch.

There are four possible LED states:

- No light
- Steady light in one of the following colors:
  - Green
  - Amber
  - Yellow (displays when both green and amber LED elements are lit)
- Slow-flashing light (green, amber, or yellow)
- Fast-flashing light (green, amber, or yellow)

The LEDs can flash green, yellow, or amber while the switch is starting or while a POST or other diagnostic tests are running. This is normal. It does not indicate a problem unless the LEDs do not indicate that all components are operational after the switch is started, after a POST, or after any diagnostic tests are complete.

See the error log for any errors. For information about the error log, see the *Brocade Diagnostic and System Error Message Reference*.

LEDs on the 16-port card

The following LEDs are on the 16-port card:

- Power LED
- Status LED
- Port status LED for each port
- Port speed LED for each port

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

Figure 26 on page 33 shows the location of the LEDs on the 16-port card.

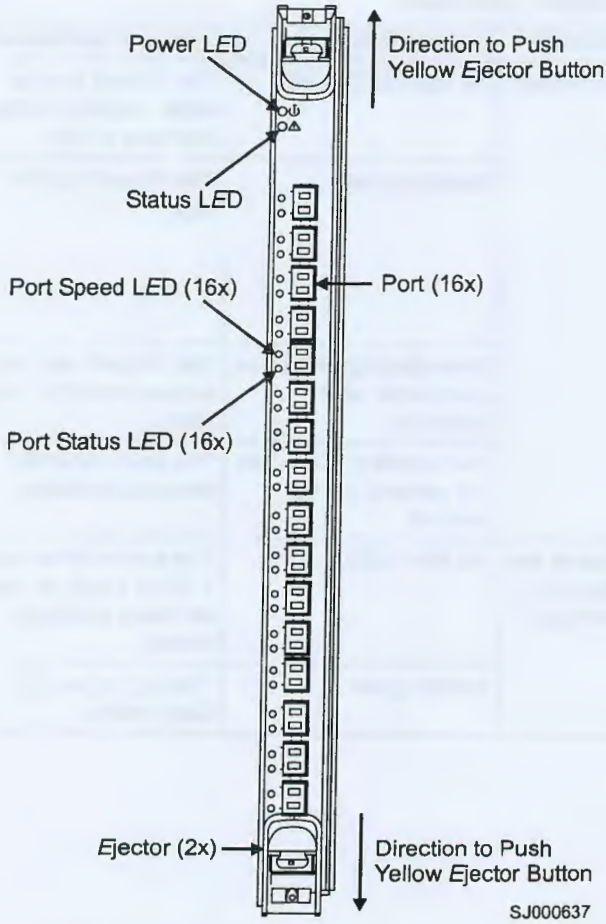


Figure 26. 16-port card LEDs

Table 3 describes the 16-port card LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and the action that you can take in response to that status.

Table 3. 16-port card LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Uppermost LED	No light (LED is off)	The 16-port card does not have incoming power.	Ensure that the card is firmly seated and has power.
		Steady green	The 16-port card has incoming power.	No action is required.

Table 3. 16-port card LED patterns (continued)

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Status	Below the Power LED	No light (LED is off)	The 16-port card is either healthy or does not have power.	Verify that the Power LED is lit.
		Steady yellow	The 16-port card is faulty.	Ensure that the card is firmly seated and check the status with the **slotShow** command. If the LED still displays yellow, contact IBM.
		Slow-flashing yellow (on 2 seconds; off 2 seconds)	The 16-port card is not seated correctly, or is faulty.	Pull the card out and reseat it. If the LED continues to flash, replace the card.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	The environmental range is exceeded.	Check for out-of-bounds environmental condition.
Port Speed	Uppermost of the two LEDs to the left of each port	No light (LED is off)	The port is either set to 1 Gbps mode, or does not have incoming power.	Verify that the Power LED is lit. To change the mode, see the *Brocade Fabric OS Procedures Guide*.
		Steady green	The port is set to 2 Gbps mode.	No action is required.

Table 3. 16-port card LED patterns (continued)

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Port Status and Activity	To the left of each port, below the Port Speed LED	No light (LED is off)	• Either the 16-port card does not have incoming power or there is no light or signal carrier detected. • Polling is in progress. • The connected device is configured in an offline state.	Verify that the Power LED is lit and check the transceiver and the cable.
		Steady green	The port is online (connected to an external device) but has no traffic.	No action is required.
		Slow-flashing green (on 1 second; off 1 second)	The port is online but segmented, indicating a loopback plug or cable, or an incompatible switch.	Verify that the correct device is connected to the port.
		Fast-flashing green (on 1/4 second; off 1/4 second)	The port is in internal loopback (diagnostic).	No action is required.
		Flickering green	The port is online, with traffic flowing through the port.	No action is required.
		Steady yellow	The port is receiving light or signal carrier, but is not yet online.	No action is required.
		Slow-flashing yellow	The port is disabled (from diagnostic tests or the **portDisable** command).	Reset the port from the workstation.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	The SFP or the port is faulty.	Change the SFP or reset the switch from workstation
		Alternating green and yellow	The port is bypassed.	Reset the port from the workstation.

LEDs on the CP card

The following LEDs are on the CP card:

- Power LED
- Status LED
- Link status and activity LED
- Link speed LED

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

10971 Fls
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 115
Doc 3698

Figure 27 shows the location of the LEDs on the CP card.

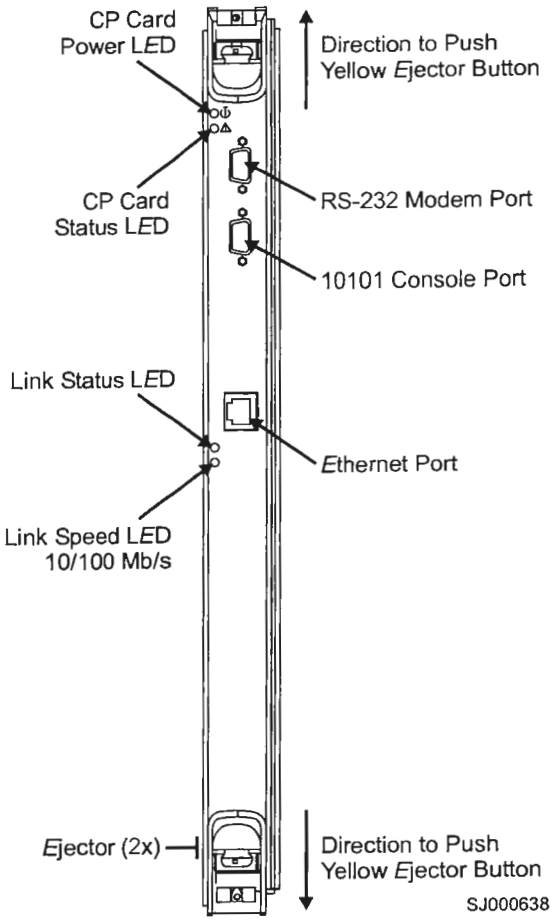


Figure 27. CP card LEDs

Table 4 describes the CP card LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and action that you can take in response to that status.

Table 4. CP card LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Uppermost LED	No light (LED is off)	The CP card does not have incoming power.	Ensure that the CP card is firmly seated and has power.
		Steady green	The CP card has incoming power.	No action is required.
Status	Below the Power LED	No light (LED is off)	The CP card is either healthy or does not have incoming power.	Verify that the Power LED is lit.
		Steady yellow	The CP card is faulty.	Ensure that the CP card is firmly seated. If the LED still displays yellow, contact IBM.
		Slow-flashing yellow (on 2 seconds; off 2 seconds)	The CP card is not seated correctly, or is faulty.	Pull the CP card out and reseat it. If the LED continues to flash, replace the CP card.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	The environmental range is exceeded.	Check for out-of-bounds environmental condition.
Link status and activity (labeled "Link" on the CP card)	Uppermost of the two LEDs below and to the left of the Ethernet port	No light (LED is off)	Either the CP card does not have incoming power or no link is detected.	Ensure that the CP card has power. Verify that the Ethernet cable is firmly seated and the device at the other end of the link is functioning.
		Flickering green and yellow	The link is healthy, with traffic flowing through the port.	No action is required.
Link speed (labeled "10/100 Mb/s" on the CP card)	To the left of the Ethernet port, below the Link status and activity LED	No light (LED is off)	Either the link speed is 10 Mbps or the CP card does not have incoming power.	Ensure that the CP card has power.
		Steady green	The link speed is 100 Mbps.	No action is required.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1150
Doc 3698

LEDs on the power supply

The following LEDs are on each power supply:

- Power LED
- Predictive Failure LED
- Fail LED

If only one ac power switch is turned on, the fail LED on each of the two power supplies without power lights up.

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

Figure 28 shows the location of the LEDs on the power supply.

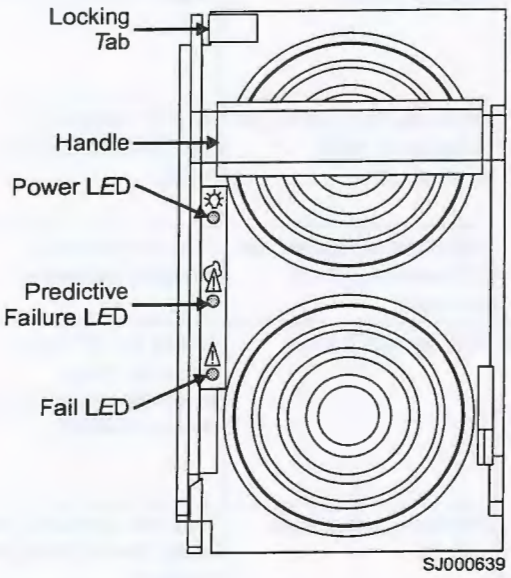


Figure 28. Power supply LEDs

Table 5 on page 39 describes the power supply LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and action that you can take in response to that status.

Table 5. Power supply LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Uppermost LED	No light (LED is off)	The power supply does not have incoming power.	Ensure the following: • The power supply is firmly seated. • The switch has incoming power. • Both power cables are connected. • The ac power switches are on.
		Steady green	The power supply has incoming power and is providing power to the switch.	No action is required.
Predictive Failure	Below the Power LED	No light (LED is off)	The power supply is either healthy or does not have incoming power.	Check the Power LED.
		Flashing amber	The power supply is about to fail because there is a failing fan inside the power supply.	Replace the power supply.
Fail	Below the Predictive Failure LED	No light (LED is off)	The power supply is either healthy or does not have incoming power.	Check the Power LED.
		Steady amber	Either the switch has power but this power supply does not (ac switch might be off), or the power supply has failed.	Ensure that the correct ac power switch is on and the power supply is seated. If the LED still displays, replace the power supply.
		Flashing amber	The power supply is unable to supply power.	Verify that the incoming power meets the requirements listed in "Power specifications" on page 103.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1167
3698
Doc

LEDs on the blower assembly

The following LEDs are on each blower assembly:

- Power LED
- Fault LED

Figure 29 shows the location of the LEDs on the blower assembly.

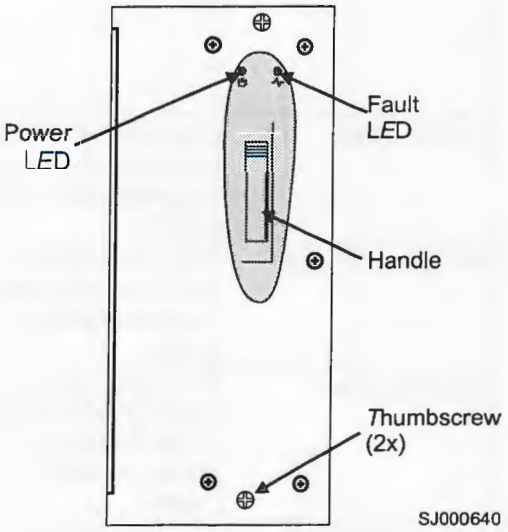


Figure 29. Blower assembly LEDs

Table 6 describes the blower assembly LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and action that you can take in response to that status.

Table 6. Blower assembly LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Above and to the left of the blower assembly handle	No light (LED is off)	The blower assembly does not have incoming power.	Ensure that the blower assembly is firmly seated and has power.
		Steady green	The blower assembly has incoming power.	No action is required.

10965 Paula

Table 6. Blower assembly LED patterns (continued)

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Fault	Above and to the right of the blower assembly handle	No light (LED is off)	The blower assembly is either healthy or does not have incoming power.	Ensure that the blower assembly has incoming power.
		Steady amber	The blower assembly has fully or partly failed.	Replace the blower assembly.
		Slow-flashing amber (on 2 seconds; off 2 seconds)	The blower assembly is not seated correctly or is faulty.	Pull out the blower assembly and reseat it. If the LED continues to flash, replace the blower assembly.
		Fast-flashing amber (on 1/2 second; off 1/2 second)	The environmental range is exceeded.	Check for an out-of-bounds environmental condition, resolve any problems, then reseat unit. If the LED continues to flash, replace the unit.

LEDs on the WWN card and bezel

The WWN card and bezel are located at the top of the chassis on the blower assembly side. The bezel covers the WWN card, allowing the LEDs to shine through. The WWN card and bezel provides a consolidated LED view of:

- The incoming power to and status of the 16-port cards in slots 1 - 4 and 7 - 10
- The incoming power to and status of the CP cards in slots 5 and 6
- The incoming power to the four power supplies

If a slot has a filler panel in place of a 16-port card, a CP card, or a power supply, the LEDs for that slot on the WWN card and bezel do not light up.

If a Status or Fail LED on the power supply flashes, the Power LED on the WWN card also flashes for increased visibility.

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

Figure 30 on page 42 shows the location of the LEDs on the WWN card and bezel.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1158
Nº Doc 3698

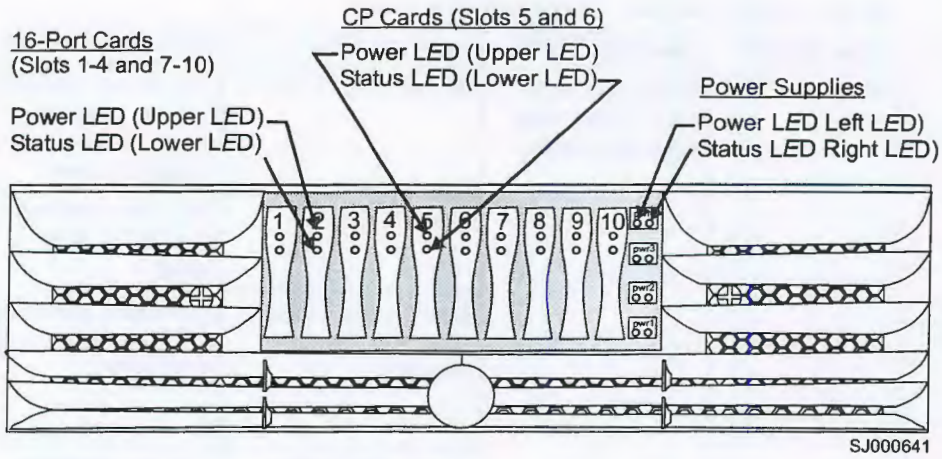


Figure 30. LEDs on the WWN card and bezel

Interpreting POST

The 2109 Model M12 performs a POST by default each time the chassis is powered on (cold start) or started. You can restart the 2109 Model M12 with the **switchReboot, reboot,** or **fastboot** commands. The **fastboot** command restarts the switches without running a POST. A CP card failover event results in a restart for the affected CP card.

POST includes a number of diagnostic tests. You can monitor the test results through LED activity, the error log, or the command line interface. POST requires a minimum of 3 minutes to complete (the time varies and depends on the devices that are connected to the 2109 Model M12).

POST includes the following steps:

1. Running preliminary POST diagnostics
2. Initializing the operating system
3. Initializing the hardware
4. Running diagnostic tests on a number of functions, including:
   - Internal connections and circuitry
   - Port function
   - Ability to send and receive frames
   - All aspects of memory, parity, and statistics counters
   - Correct serialization

The following switch initialization steps are performed whether or not a POST runs:

1. Configures the universal port.
2. Initializes the links.
3. Analyzes the fabric. If any ports connect to other fabric elements (switches), the switch participates in a fabric configuration.
4. Obtains a domain ID and assigns port addresses.
5. Constructs unicast routing tables.
6. Enables normal port operation.

Perform the following steps to verify that a POST completes without errors:

1. Verify that all LEDs return to a normal state after a POST completes. If one or more LEDs do not return to a normal state, and this is not due to the switch being set to beacon, see "Interpreting LED activity" on page 32. Run the **slotShow** command to check the status of the slots.
2. Verify that the switch prompt displays when a POST completes. If it does not display, a POST did not successfully complete. Contact IBM for support.
3. Review the system log. Any errors that are detected during a POST are written to the system log. You can view this error log by running the **errShow** command.

For information about error messages or how to set a switch to beacon, see the *Brocade Diagnostic and System Error Message Reference* and the *Brocade Fabric OS Reference*.

Maintaining the switch

The 2109 Model M12 does not require any regular physical maintenance. It is designed to minimize the chance of failure by using diagnostic tests and field replaceable units (FRUs).

Diagnostic tests

Diagnostic tests are provided to help you to identify problems in the hardware and the firmware. The diagnostic tests include tests of internal connections and circuitry, SFPs, and fiber-optic cables in use. You can run the tests either by using Telnet or through a terminal that is set up for a serial connection to the switch. Some tests require that external cables connect the ports to each other. This allows diagnostics to verify the serializer or deserializer interface and to test the attached SFP and cable.

All diagnostic tests run at link speeds of 1 Gbps and 2 Gbps. For information about diagnostic tests and how to run them, see the *Brocade Fabric OS Reference*.

Note: The diagnostic tests temporarily lock the transmit and receive speed of the links to a specific speed.

Field replaceable units

You can replace the 16-port cards, CP cards, power supplies, and blower assemblies in the field without special tools. In most cases, the switch can continue to operate while you replace a field replaceable unit (FRU). See Chapter 7, "Servicing the 2109 Model C36 with Model M12", on page 69 for the detailed procedures for how to replace these FRUs and other components.

You can configure Fabric Watch alarms for each FRU. For information about Fabric Watch alarms, see the *Brocade Fabric Watch User's Guide*.

You can determine the status of the individual FRU by visually checking the LEDs on the hardware components (see "Interpreting LED activity" on page 32) or by using Telnet commands. For information about Telnet commands, see the *Brocade Fabric OS Reference*.

Environmental status and maintenance commands

You can also view environmental information and switch status by using Telnet commands. See the *Brocade Fabric OS Reference* for a complete description of these commands.

Chapter 5. Installing modems

Each CP card in the 2109 Model M12 contains a modem serial port that allows you to connect to a Hayes-compatible modem. The modem serial port is wired as a standard DTE port. You do not need any additional software on the 2109 Model M12 to use the modems.

The modem serial port has the same command, login capabilities, and operational behavior as the terminal serial port. However, asynchronous informational messages and other unsolicited text are not sent to the modem ports.

Connecting a separate modem to each CP card and then connecting both modems to a shared telephone line ensures the high availability of the modem connection. This ensures that one telephone line is used to access the active CP card when a failover occurs. You must log in again if a failover occurs. If both CP cards connect to a shared telephone line, callers automatically dial into the active CP card. The active CP card answers on the first ring. If the active CP card cannot answer for any reason, the standby CP card answers on the seventh ring and allows a login to proceed.

Note: The 2109 Model M12 detects modems only during power-on, restart, or a CP card failover sequence.

After you connect the modems, you can use a Telco system to dial-in to the modems and verify that they answer and dialogue as expected. If a dial-out modem facility is not available, you can use a terminal emulation program on a computer workstation (or laptop) that has an attached modem. See "Setting up a remote modem system (optional)" on page 46 for instructions on how to set up a remote modem for testing purposes. For security reasons, the modem session is automatically disconnected if the modem cable is detached while a session is active.

Figure 31 on page 46 shows two modems that are connected to a 2109 Model M12.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 3698
Doc.

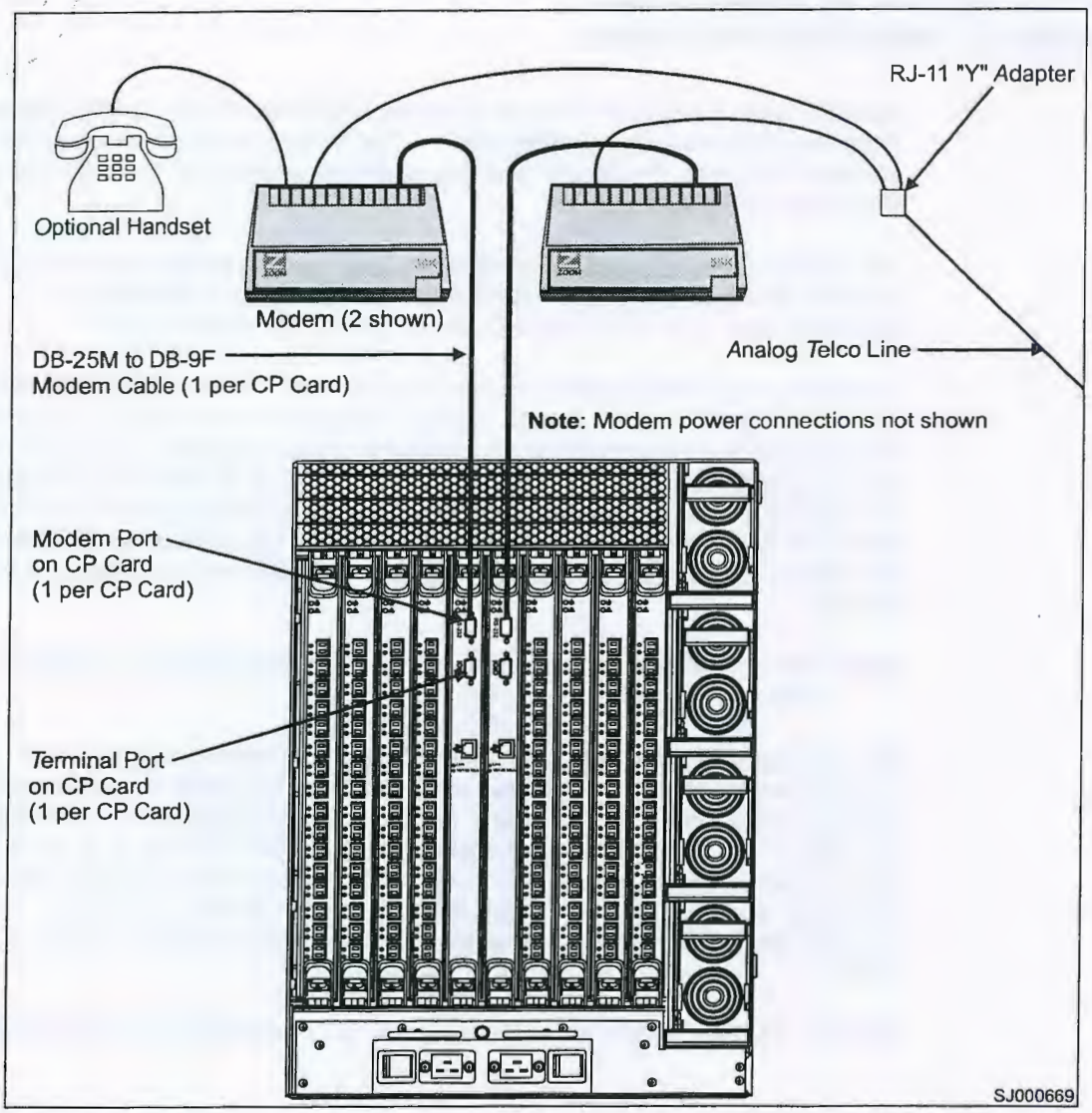


Figure 31. 2109 Model M12 with two modems connected

Setting up a remote modem system (optional)

Note: You should set up the modems before you power on the 2109 Model M12 and connect it to the fabric.

This section provides information about how to set up a remote modem for testing the 2109 Model M12 modems.

Perform the following steps to set up the optional remote modem system:

1. Connect the remote modem to a computer workstation that has a terminal emulator application such as HyperTerminal on Windows 95, 98, 2000, ME or NT, or TERM in a UNIX environment.
2. Disable any serial communication programs that are running on the workstation, such as synchronization programs for a personal digital assistant (PDA).

3. Start the terminal emulator application and if needed, configure as follows:
   - Enter the parameters in Table 7 for Windows 95, 98, 2000, ME, or NT, or TERM in a UNIX environment.

Table 7. Modem parameters for Windows 95, 98, 2000, ME, or NT, or TERM in a UNIX environment

Parameter	Value
Port speed (bits per second)	115200. This value usually defaults to the highest speed that the modem supports and then possibly negotiates for a slower speed.
Data protocol	Standard EC
Compression	Enabled
Flow control	Hardware
Databits	8
Parity	None
Stop bits	1
Modulation	Standard

   - For most UNIX systems, at the prompt, type:

     ```
     tip /dev/ttyb -9600
     ```

4. Follow the instructions from the modem manufacturer for setting up and verifying the modem operation.

Installing the modems on the 2109 Model M12

Note: You should set up the modems before you power on the 2109 Model M12 and connect it to the fabric.

The 2109 Model M12 detects modems only during power on, restart, or CP card failover. Set up the modems before you connect the 2109 Model M12 to the fabric.

You need the following items to set up two modems to work with the 2109 Model M12:

- Two Hayes-compatible modems, such as the Zoom/Modem V.92 EXT Model 3049
- Two standard modem cables, DB25 (male) to DB9 (female)
- One RJ-11 Y adapter for standard Telco wiring or equivalent circuitry (a total of three connections)
- One analog telephone line

CAUTION:
For normal installation, the 2109 Model M12 and attached modems are powered off before cabling them. The modems are automatically detected during a power-on sequence.

Perform the following steps to install the modems:

1. Verify that the power to the 2109 Model M12 is off.
2. Set up the two modem units and the required power connections. Do not turn on the power to the modems until all cables are attached.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1161
Doc. 3698

3. Connect the modem cables to the modems and to the 2109 Model M12 modem ports. See Figure 31 on page 46.
4. Connect the telephone line inputs on the modems to the RJ-11 *Y* adapter. This effectively places both modems on a single telephone line.
5. Optional: Connect a telephone handset to one of the telephone connections on the modem. See Figure 31 on page 46.
6. Connect the RJ-11 *Y* adapter to an appropriate analog telephone line.

   Note: Write down the dial-in number. You will use this number later.
7. Turn on the power to the modems. Verify that the modem-ready (MR) indicators light on both modems.
8. Power on the 2109 Model M12, or restart it if you did not power off during the previous steps. Performing this step allows the 2109 Model M12 to recognize the modems.

Verifying modem installation

Perform the following steps to verify that the modems are installed correctly:

1. Verify that both modem cables are connected at the modem and the CP card.
2. Turn on the power to the modems if not already on.
3. Turn on the power to the 2109 Model M12 if not already on.
4. Verify that both modems are ready by checking the following LEDs:
   - Clear to send (CS)
   - Terminal ready (TR)
   - Modem ready (MR)

   If the LEDs do not light, ensure that the modems are connected to a power source and have the power turned on. Also recheck the modem cable connections on the modem and the modem port of the 2109 Model M12.
5. Wait until a POST completes on the 2109 Model M12 (a minimum of 3 minutes).
6. Using a remote client dialing facility (as described in "Setting up a remote modem system (optional)" on page 46), dial in to the customer telephone number for the 2109 Model M12.
7. Observe the modem LEDs. The ring indicator (RI) LED should flash briefly as the telephone rings. If the RI LED does not flash on both modems, recheck the incoming telephone lines to the modems.
8. After one ring, the off hook (OH) LED on the modem that is associated with the active CP card (usually in slot 5) should light. A login prompt displays to the remote client. Login normally.

   Note: If the OH LED on the standby CP card (usually in slot 6) lights after seven rings, recheck the active modem cable connections of the CP.
9. Disconnect the modem session of the active CP card that is using the remote client software.
10. Remove the Telco connector from the active CP card modem. Leave the Telco line of the standby CP card connected to the RJ-11 *Y* adapter. See Figure 31 on page 46.
11. Using the remote client dialing facility, dial in to the customer telephone number for the 2109 Model M12.

12. Observe the modem LEDs carefully. The RI LED should now flash only on the modem that is connected to the standby CP card.
13. After seven rings, the OH LED on the modem that is associated with the standby CP card should light. A login prompt displays to the remote client. A message confirms that the standby CP card is being logged into. Login normally, if desired, or disconnect the session.
14. Restore the Telco connector to the active CP card modem.

The 2109 Model M12 modems are now ready to use.

Notes:

1. Experienced users can use the **haFailover** command to further evaluate the attached modems. It is important to wait approximately 5 minutes after a failover (or restart) to allow the system to correctly set up the modems.
2. For security reasons, the modem session is disconnected if the modem cable is detached while a session is active.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1162
Doc. 3698

10956 Paula

Chapter 6. Installing and removing an additional 2109 Model M12

This chapter describes how to install and remove an additional 2109 Model M12 from a Model C36 cabinet.

Installation considerations and safety guidelines

DANGER

A fully populated 2109 Model M12 weighs approximately 115 kg (250 lbs) and requires a minimum of two people and a lift tool to install it. Before you install it, verify that the additional weight of the chassis does not exceed the cabinet's weight limit or unbalance the cabinet. When you calculate the additional weight, include the cards or power supplies that partially extend out of the chassis.

Attention: To ensure adequate cooling, install the chassis with the port side facing the aisle where exhaust air is released (usually called the service aisle). This prevents the fans from pulling in heated exhaust air.

Before you install an additional 2109 Model M12 into the cabinet, perform the following tasks:

- Ensure that a space that is 14U high, 74 cm (29 in.) deep, and 48 cm (19 in.) wide is available in the cabinet.
- Ensure that there is a minimum distance of 71.75 cm (28.25 in.) between the front and back rails of the cabinet.
- Verify that the additional weight of the chassis does not exceed the weight limit of the cabinet.
- Ensure that all equipment that is installed in the cabinet is grounded through a reliable branch circuit connection. Do not rely on a secondary connection to a branch circuit, such as a power strip.
- Plan for managing the cables before you install the chassis. You can manage the cables in a variety of ways, such as:
  - Routing the cables below the chassis
  - Routing the cables to either side of the chassis
  - Routing the cables through the cable channels on the sides of the cabinet
  - Using the patch panels
- Ensure that the power directors have two dedicated electrical branch circuits with the following characteristics available for use:
  - 200 - 240 V ac, 30 amps
  - 50 - 60 Hz
- Ensure that the two dedicated electrical branch circuits are protected with a circuit breaker that is in accordance with the local electrical codes.
- Ensure that the supply circuit, line fusing, and wire size are adequate according to the electrical rating on the chassis nameplate.
- Ensure that a licensed electrician installs the grounded outlets and that they are compatible with the power cords.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1163
Doc 3698

- Ensure that the 2109 Model M12 has access to a minimum airflow of 350 cubic feet per minute.
- Ensure that the air temperature that is measured at the blower inlet does not exceed 40°C (104°F) during operation.

Ordering the lift tool

The ordering procedures are different for the lift tool and depend on your location. You should direct questions about these procedures to your regional specialist.

Note: The bridge tool (PN 18P5855), which is required for installation, is shipped with a new or a replacement 2109 Model M12. The bridge tool, when installed, serves as a temporary ramp between the lift tool and the 2109 Model M12 rails that are installed in a Model C36 cabinet. You do not need to return the bridge tool when you are done with it.

World trade locations

The following ordering procedures are for world trade locations:

- Order the lift tool by using the parts order system, like any other part.
- Use the following part numbers when you order:
  - Lift tool: PN 09P2481
  - 24-inch load plate: PN 11P4369
- You do not record parts usage.
- Return the lift tool and the 24-inch load plate to the parts center after you complete the installation or removal of the 2109 Model M12.

United States locations

In the United States, call UPS Logistics at 800-528-6046 to order the lift tool and the 24-inch load plate.

Note: For the SSR branch and territory, the United States cannot order the lift tool or 24-inch load plate through the parts order system. UPS Logistics are used to ship and return the lift tool and 24-inch load plate.

Use the following part numbers when you order:

- Lift tool: PN 09P2481
- 24-inch load plate: PN 11P4369

Note: When you order the lift tool, you will receive an 18-inch load plate. Do not use the 18-inch load plate. You must order and use a 24-inch load plate when you install the 2109 Model M12.

You must provide the following information when you order the lift tool. This information is necessary to ensure that the lift tool is delivered when you need it. Failure to provide this information might delay the completion of the order request and the shipping request. It might also result in a time and date to return the tool that is different from what you need.

- Phone number and customer contact
- Account code: 98577
- Time and date of delivery
- Accurate destination address with zip code
- Time and date of return pickup

You must return the lift tool at the time that was scheduled with UPS Logistics. If you need to change the scheduled return time or date, contact UPS Logistics.

You are responsible for ensuring that all of the paperwork and components are packed and restored in the arbocrate (shipping container) of the lift tool. Ensure that the tool is functioning properly before you release the tool to UPS Logistics for return. You are accountable for the tool until UPS Logistics picks up the lift tool for return delivery to their parts storage facility.

Contact your branch office tools coordinator or your region specialist if you have any questions or concerns.

2109 Model M12 standard shipment

A 2109 Model M12 is shipped with the following items:

- The 2109 Model M12, which includes:
  - Four to eight 16-port cards (customer-specified configuration)
  - Two CP cards
  - Four power supplies
  - Three blower assemblies
- One accessory kit that contains the following items:
  - *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*
  - 2109 Model M12 documentation CD-ROM
  - ESD grounding strap
  - One 3.05 m (10 ft) RS-232 serial cable with an RJ-45 style adapter on the end of the cable
  - The 14U chassis mount kit with installation instructions
  - Bridge tool: PN 18P5855

Note: You can order SFP transceivers separately from IBM. The 2109 Model M12 supports both SWL and LWL transceivers.

Unpacking the 2109 Model M12

Perform the following steps to unpack the 2109 Model M12.

Note: This procedure requires a 1/2-in. socket wrench to remove the pallet bolts.

1. Remove the upper portion of the packing crate while the switch is still in the shipping area to reduce clutter at the installation site.
   a. Open the latches that hold the top of the crate to the pallet. To open a latch, pull the handle out, turn it to the left, then slide the latch open.
   b. Lift the top of the crate off the pallet.
   c. Leave the foam on top of the chassis to hold the kits in place during transportation to the installation area.
   d. Do not move the chassis off the pallet until the door is removed.
2. Open the shipping crate by pulling the handle of the latch and turning it counterclockwise. Slide the latch open.
3. Remove the packing foam, antistatic plastic, 14U chassis mount kit, and accessory kit.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1161
Doc. 3698

4. Unscrew the four bolts that hold the 2109 Model M12 to the pallet. See Figure 32. Remove the brackets.

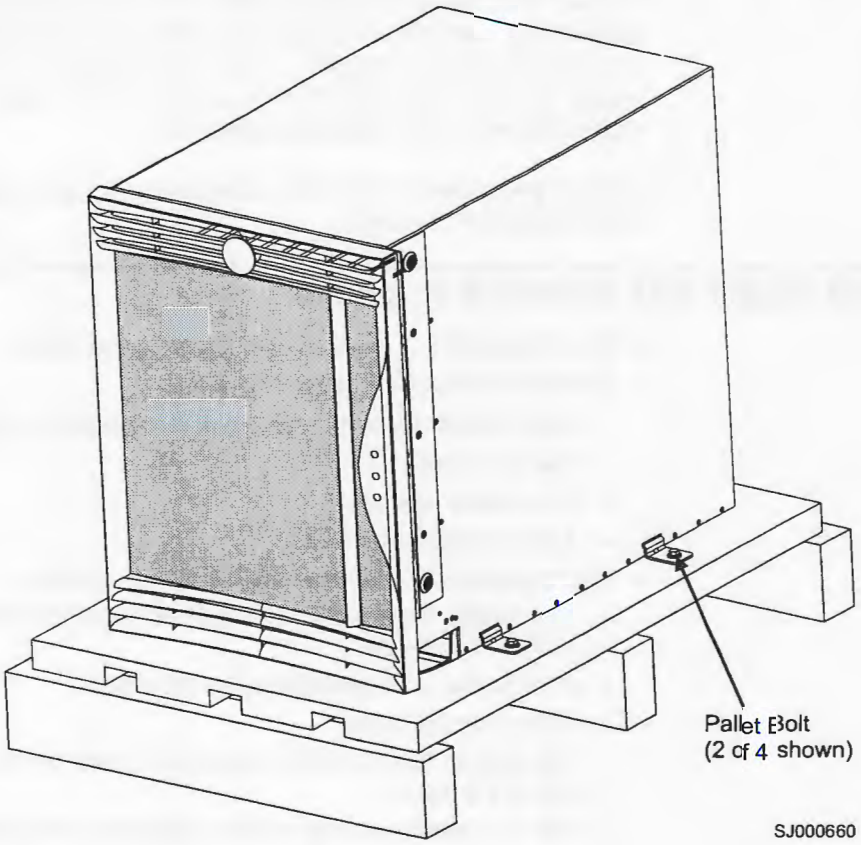


Figure 32. 2109 Model M12 on a pallet

Attention: Remove the chassis door before you move the chassis.

5. Remove the chassis door from the chassis.
   a. Open the door 90°.
   b. Support the door to prevent it from falling. Pull the door away from the chassis.
   c. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge. See Figure 33 on page 55.
   d. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge. Pull the door out, towards you.
   e. Pull the door away from the chassis.

10952 Paula

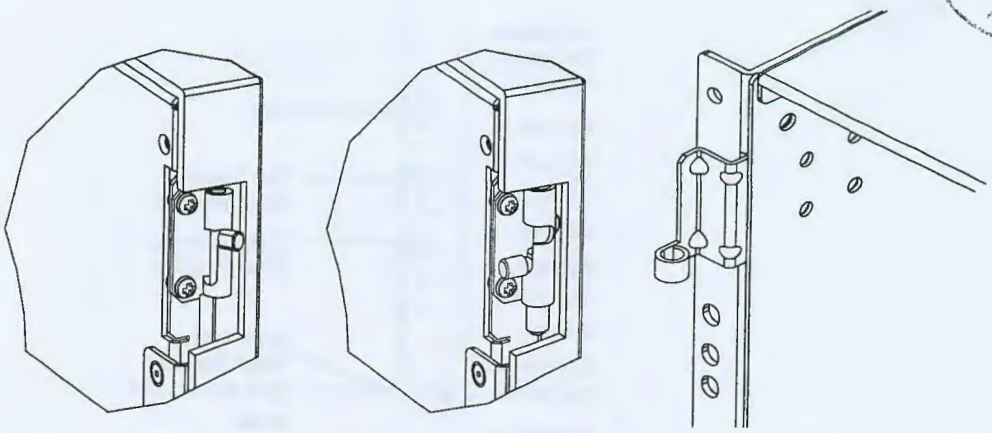


Figure 33. Removing the chassis door

Installing the 2109 Model M12 in the cabinet

This section describes how to install the 2109 Model M12 in the Model C36 cabinet. These procedures use parts that are included in the 14U chassis mount kit. See Table 23 on page 115 for a list of these parts.

Time required

Allow approximately 2.5 hours to complete this procedure. This includes unpacking, assembling, and repacking the lift tool.

Note: Assembly instructions for the lift tool are in the shipping container.

Tools required

You will require the following items to install the 2109 Model M12 in the cabinet:

- #2 Phillips screwdriver
- Lift tool

Installing the brackets

Perform the following steps to install the brackets:

1. Loosen the adjusting screws on the left and right mount shelf brackets to allow for adjustment to the cabinet depth.
2. Attach the left and right mount shelf brackets to the rails in the cabinet. Standard EIA rail spacing of holes is sets of three, separated by 5/8 in., 5/8 in., and 1/2 in. See Figure 34 on page 56.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1165
Doc. 3698

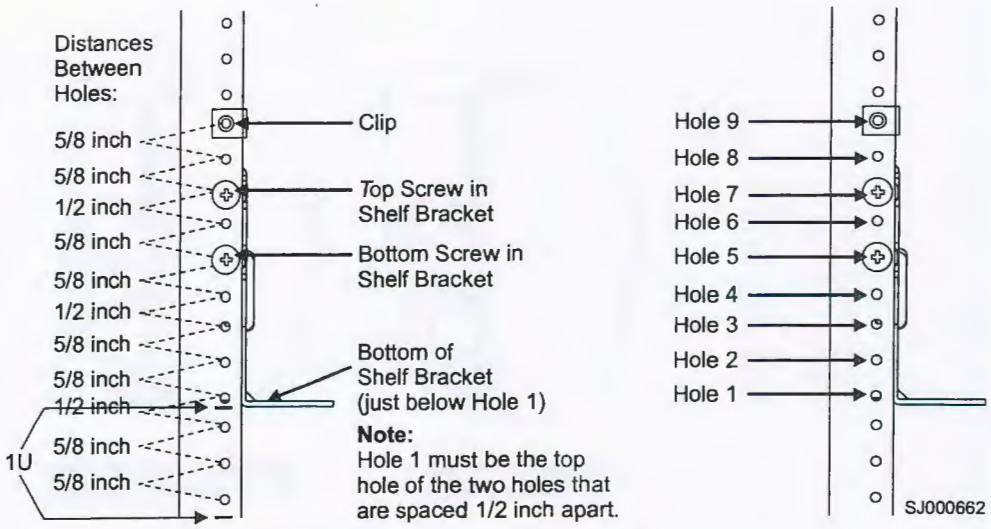


Figure 34. Placement of the shelf brackets and clip nuts on the cabinet rails

Note: If you are installing a 2109 Model M12 into the bottom of the rack, go to step 2a for the location of the rail. If you are installing a 2109 Model M12 into the top of the rack, go to step 2b for the location of the rail.

a. Locate the screws in the middle of EIA unit 5 and the bottom of EIA unit 6 for the back of the cabinet. Locate the screws in the middle of EIA unit 4, the bottom of EIA unit 5, the middle of EIA unit 5, and the bottom of EIA unit 6 for the front of the cabinet.

b. Locate the screws in the middle of EIA unit 22 and the bottom of EIA unit 23 for the back of the cabinet. Locate the screws in the middle of EIA unit 21, the bottom of EIA unit 22, the middle of EIA unit 23, and the bottom of EIA unit 23 for the front of the cabinet.

c. You can route the cables down through the cable management tray or through the holes in the sides of the chassis. If you route the cables down through the cable management tray, allow adequate space below the chassis for cable management.

Orient the left and right mount shelf brackets with the notched portion toward the service aisle. Attach the shelf brackets to the cabinet rails, by using six 1/4-20 x 1/2-in. Phillips panhead screws with lock washers per bracket. Tighten the screws. See Figure 35 on page 57.

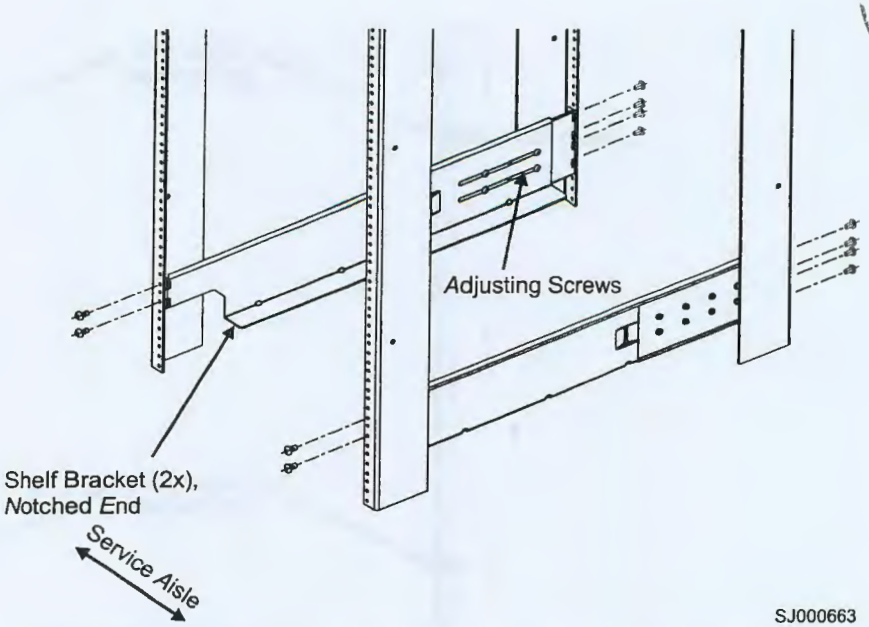


Figure 35. Shelf brackets are installed on the rails (cabinet walls are not shown)

3. Tighten the adjusting screws on the shelf brackets.
4. Attach four 10-32 clip nuts to the two rails at the front of the cabinet (service aisle side). See Figure 36 on page 58.

   Note: If you are installing a 2109 Model M12 into the bottom of the rack, go to step 4a for the location of the clip. If you are installing a 2109 Model M12 into the top of the rack, go to step 4b for the location of the clip.

   a. Attach the lower clip nuts to the top of EIA unit 6. Attach the upper clip nuts to the middle of EIA unit 17.
   b. Attach the lower clip nuts to the top of EIA unit 23. Attach the upper clip nuts to the middle of EIA unit 34.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1160
Doc. 3698

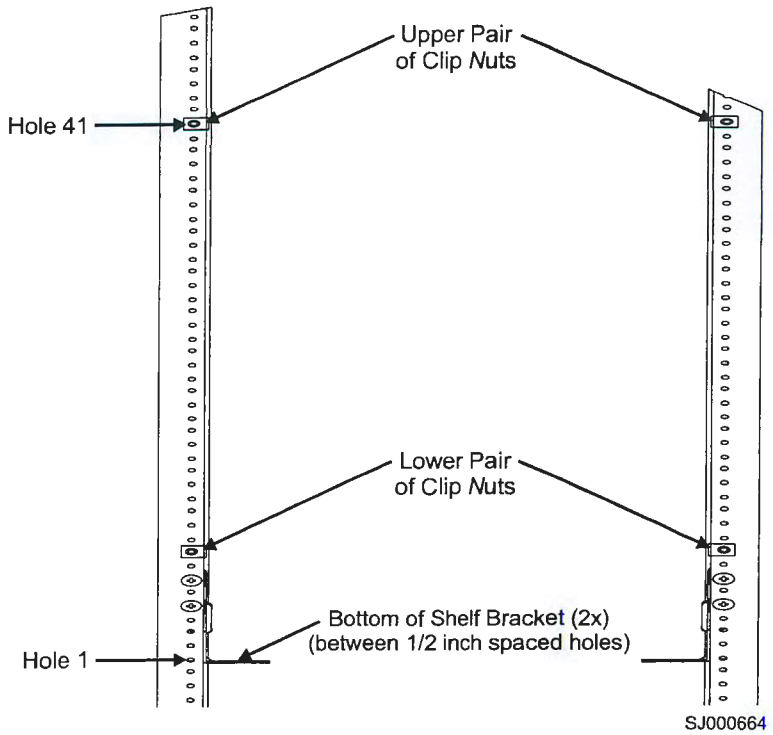


Figure 36. Placing the clip nuts on the rear rails (service aisle side)

5. Disassemble the left and right upper mount bracket assemblies. Save the screws for later use.
6. **Attention:** When you insert screws into the chassis, use the exact screws specified in the procedure. Use of longer screws might damage the chassis.

   Attach the right and left flat upper mount brackets (see Figure 37 on page 59, items 3a and 4a) to the chassis by using four of the 10-32 x 5/16-in. Phillips-flathead screws (item 5) per bracket. Tighten the screws. Orient the slotted holes in the brackets towards the blower side of the chassis. See Figure 37 on page 59 for orientation.

ECT 10948 Paula

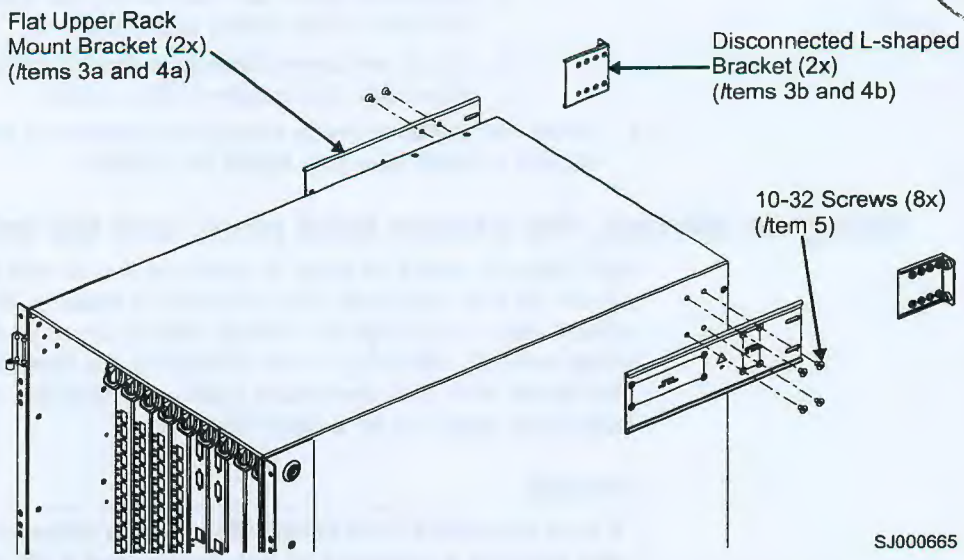


Figure 37. Attaching the right and left flat upper mount brackets to the chassis

7. Attach the two L-shaped upper mount brackets (items 3b and 4b) to the cabinet rails. See Figure 38 for orientation. Use two of the 1/4-20 x 1/2 in. Phillips panhead screws with lock washers per bracket. Tighten the screws.

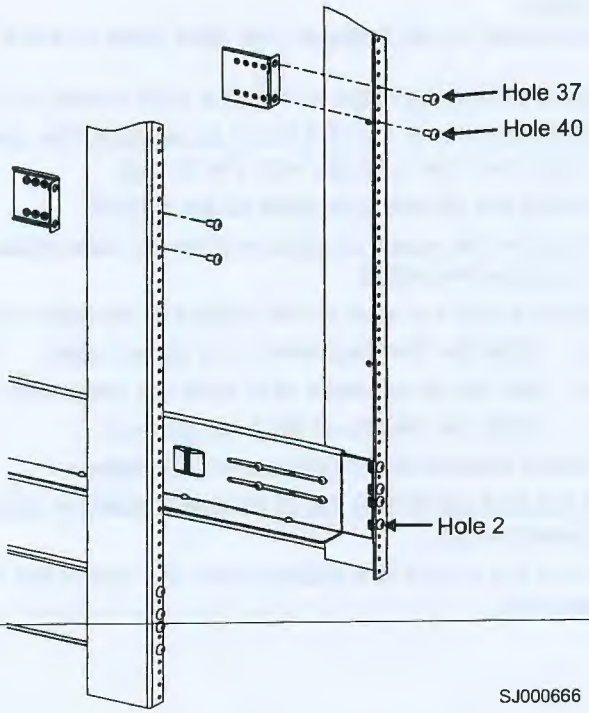


Figure 38. Attaching the L-shaped upper mount brackets to the rails

Note: If you are installing a 2109 Model M12 into the bottom of the rack, go to step 7a on page 60 for the location of the bracket. If you are installing a 2109 Model M12 into the top of the rack, go to step 7b on page 60 for the location of the bracket.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 116
Doc. 3698

a. Attach the lower clip nuts to the top of EIA unit 6. Attach the upper clip nuts to the middle of EIA unit 17.
b. Attach the lower clip nuts to the top of EIA unit 23. Attach the upper clip nuts to the middle of EIA unit 34.

8. Route the cables or cords through the cabinet or along any other route that is difficult to reach after you install the chassis.

Using the lift tool, the 24-inch load plate, and the bridge tool

Step 1through step 9 on page 61 describe how to use the lift tool (PN 09P2481) and the 24-inch load plate (PN 11P4369) to install a 2109 Model M12 in the cabinet. Step 10 on page 61 through step 21 on page 64 describe how to install the bridge tool (PN 18P5855) in the cabinet for the lower 2109 Model M12 or the upper 2109 Model M12. This procedure uses parts from the 14U chassis mount kit. See Table 23 on page 115 for a list of these parts.

DANGER

A fully populated 2109 Model M12 weighs approximately 115 kg (250 lbs) and requires a minimum of two people and a lift tool to install it. Before you install it, verify that the additional weight of the chassis does not exceed the cabinet's weight limits or unbalance the cabinet. When you calculate the additional weight, include the cards or power supplies that partially extend out of the chassis.

CAUTION:
A pinch point exists between the load plate and the bridge tool.

Perform the following steps to install a 2109 Model M12:

1. Assemble the lift tool if it is not assembled. The assembly and disassembly instructions are included with the lift tool.
2. Attach the 24-inch load plate to the lift tool.
3. Remove the power supplies and blower assemblies from the 2109 Model M12 to reduce the weight.
4. Move the lift tool next to the pallet that contains the 2109 Model M12.
   a. Adjust the load platform to the same height.
   b. Slide the 2109 Model M12 from the pallet onto the load platform.
   c. Center the switch on the load platform.
5. Attach the retention straps around the drawer.
6. If the load platform is not at its lowest position, lower the load platform to its lowest position.
7. Move the lift tool to a position near the rear of the cabinet. See Figure 39 on page 61.

ECT 10946 Paulce

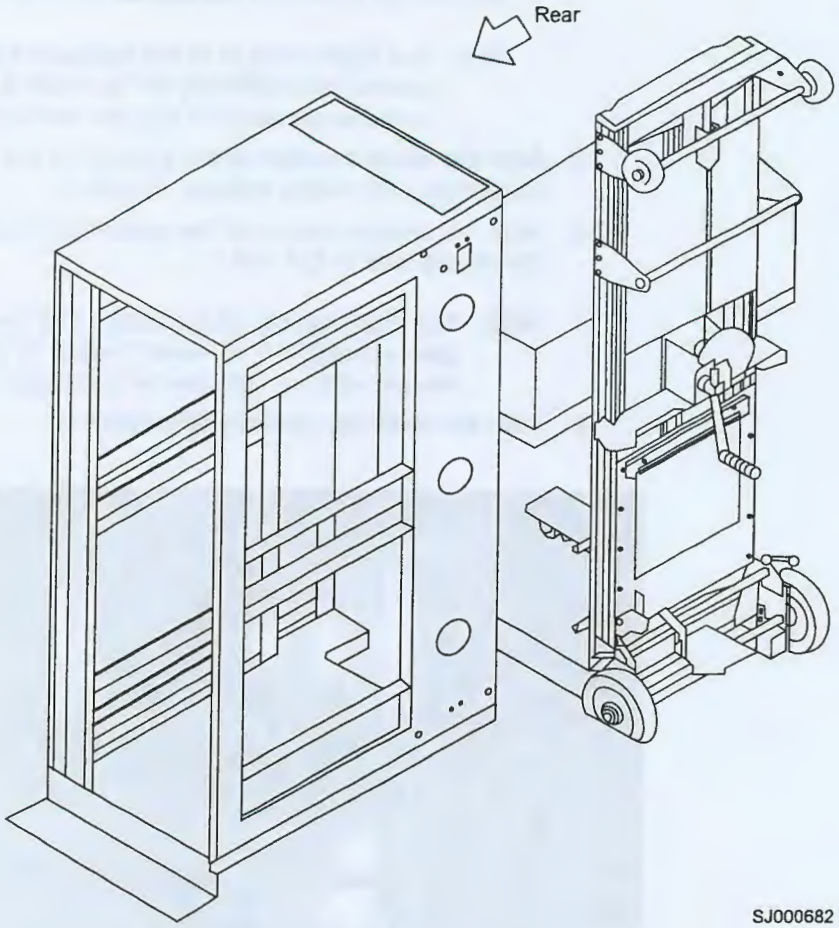


Figure 39. Rear view of cabinet and lift tool

Note: If you are passing through a narrow passage or door, it might be necessary to rotate the drawer on the load platform.

8. Set the wheel brake by pressing down on the wheel brake pedal.
9. Locate the anti-tips bars. If they are not attached, attach them to the lift tool by performing step 9a through step 9d. If the anti-tip bars were previously attached, go to step 10.
   a. Pull up on the leg lock pins and insert the anti-tip bars inside the legs.
   b. Pull on the legs and anti-tip bars to ensure that they are locked into position.
   c. Raise the platform to allow enough room to attach the anti-tip bracket.
   d. Secure the anti-tip bars by using the anti-tip bracket and bolt.
10. If you are installing the lower 2109 Model M12, go to step 11. If you are installing the upper 2109 Model M12, go to step 12 on page 62.
11. For the lower 2109 Model M12, install the bridge tool by completing the following steps:
    a. Remove the bridge tool from the box and adjust the two supports 45°.
    b. Hold the bridge tool between the two vertical supports near EIA unit 3, and move the two supports another 45°. Make sure that the following conditions are met:
       - The two-pin section of the support is on the back of the vertical support.

RQS nº 03/2005 - CN CPMI - CORREIOS
Doc. 3698

- The one-pin section of the support is on the front of the vertical support.

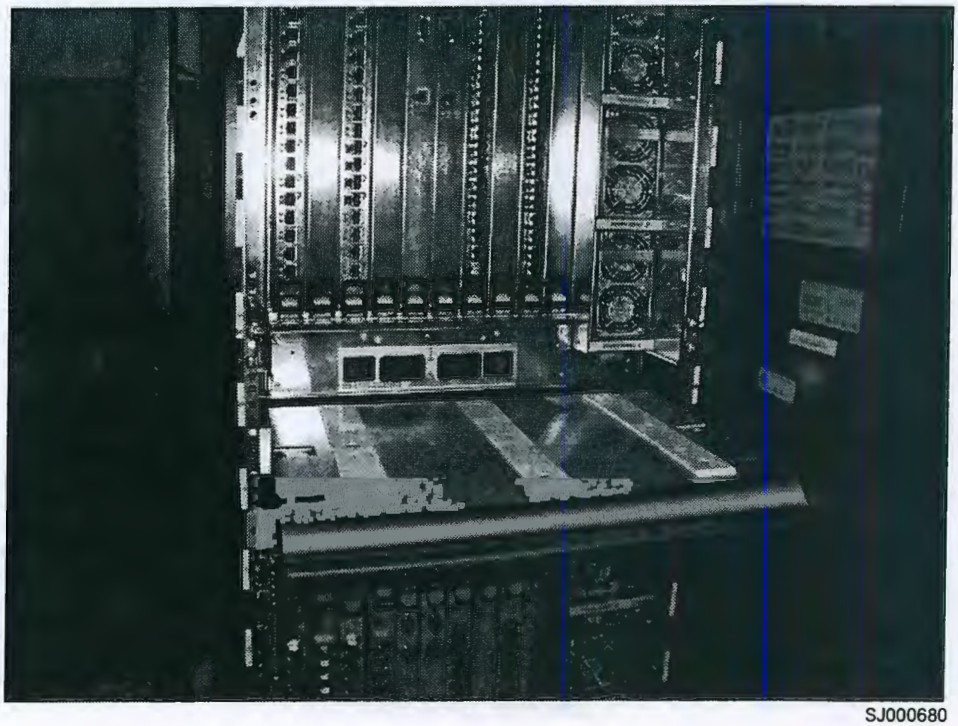
  Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and one-pin sections with the vertical support.

c. Align the two-pin section of the support on the back of the vertical rail with the bottom and middle holes in EIA unit 3.

d. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 1.

   Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and the one-pin sections with the vertical support.

e. Lock the shelf into position. See Figure 40.



SJ000680

Figure 40. Locking the shelf into position

12. For the upper 2109 Model M12, install the bridge tool by completing the following steps:

    a. Remove the bridge tool from the box and adjust the two supports 45°.

    b. Hold the bridge tool between the two vertical supports near EIA unit 20, and move the two supports another 45°. Make sure that the following conditions are met:

       - The two-pin section of the support is on the back of the vertical support.
       - The one-pin section is on the front of the vertical support.

       Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and one-pin sections with the vertical support.

c. Align the two-pin section of the support on the front of the vertical rail with the bottom hole and the middle hole in EIA unit 20.

d. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 18.

13. Turn the winch crank counterclockwise, 1/4 turn, to set the winch brake.
14. Set the wheel brake and place the wheel chocks around the wheels.
15. Remove the retention straps.
16. Slide the switch into the cabinet.
17. Remove the wheel chocks, release the wheel brake, and move the lift tool away from the cabinet.
18. Reinstall the power supplies and blower assemblies.
19. Fasten the two flat left and right upper mount brackets that are on the chassis to the two L-shaped upper left and right cabinet mount brackets. Use the two screws that were set aside in step 5 on page 58. Tighten the screws. See Figure 41.

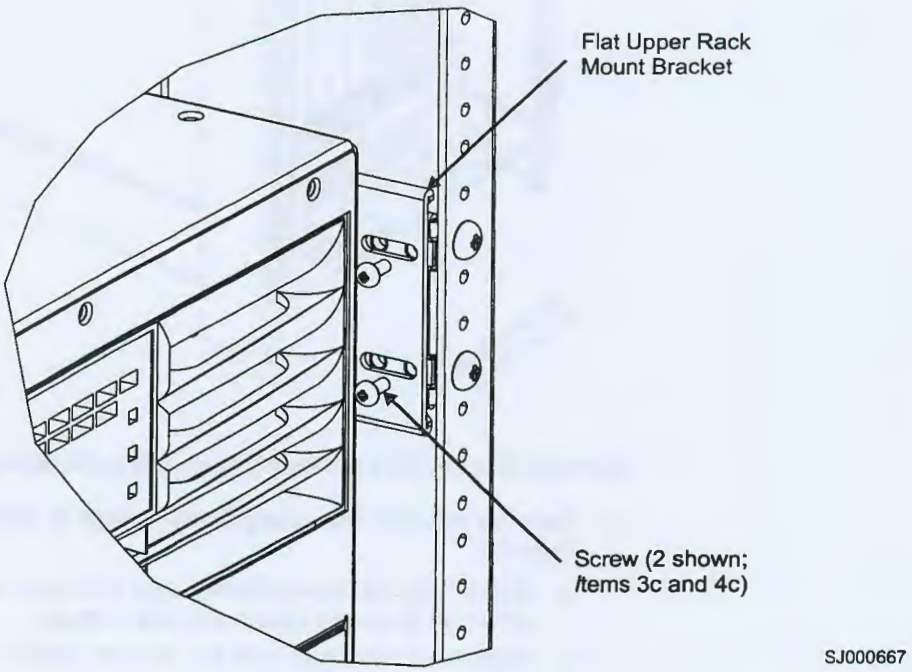


Figure 41. Attaching the mount brackets to the cabinet rails

20. Fasten the port side of the chassis to the cabinet rails. Use two of the 10-32 x 5/8-in. Phillips panhead screws with washers on each side. Tighten the screws. See Figure 42 on page 64 for the location of the screws.

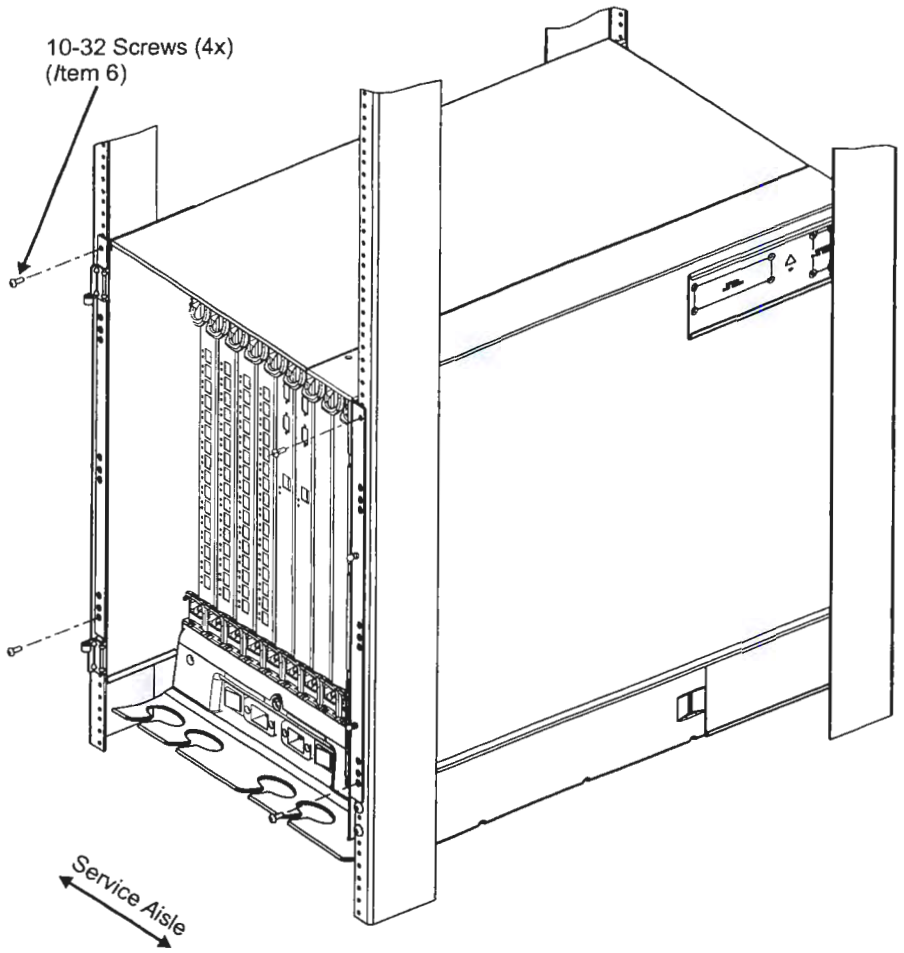


Figure 42. Attaching the port side of the chassis to the cabinet rails

21. Reinstall the door after you put the chassis in place. See Figure 43 on page 65.
    a. Ensure that the spring-loaded pins that are on both door hinges are retracted. Push the levers into the notches.
    b. Align the door hinges with the chassis portion of the hinges.
    c. Release the pins by pushing the levers out of the notches.

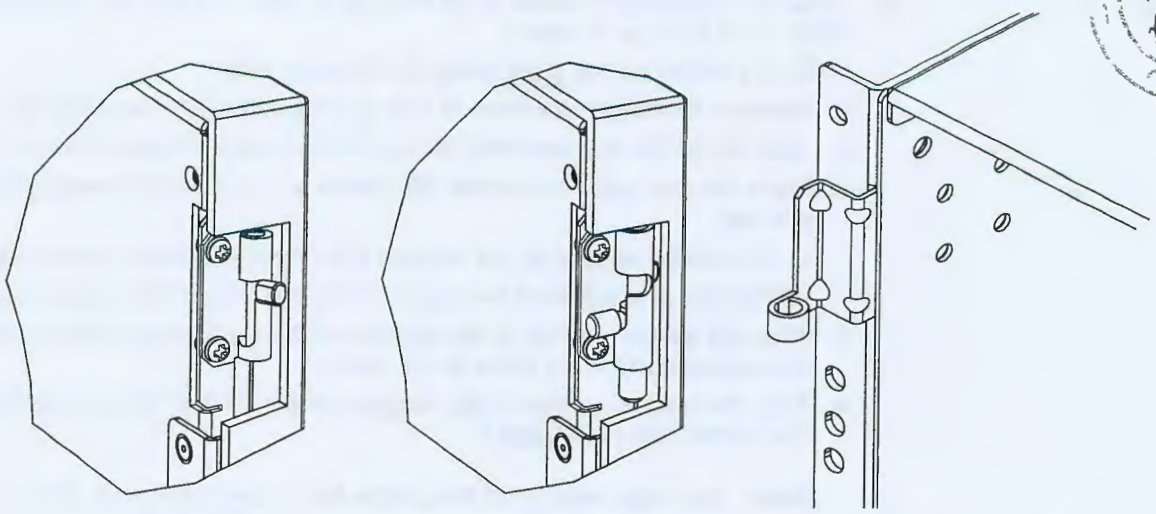


Figure 43. Removing the chassis door

22. Uninstall the bridge tool and return it to its original box.

Note: For turning on the power and for the configuration instructions, see Chapter 3, "Starting and configuring the 2109 Model M12", on page 19.

Attention: Do not connect the switch to the network until the IP addresses are correctly set.

Removing a 2109 Model M12 from the cabinet

Step 1 through step 5 describe how to use the lift tool (PN 09P2481) and the 24-inch load plate (PN 11P4369) to remove a 2109 Model M12 from the cabinet. Step 6 on page 66 through step 17 on page 67 describe how to remove the bridge tool (PN 18P5855) from the cabinet for the lower 2109 Model M12 or the upper 2109 Model M12.

Perform the following steps to remove a 2109 Model M12:

1. Assemble the lift tool if it is not assembled. The assembly and disassembly instructions are included with the lift tool.
2. Remove both power cords from the 2109 Model M12.
3. Remove the power supplies and blower assemblies from the 2109 Model M12 to reduce the weight.
4. Remove the chassis door from the chassis.
   a. Open the door 90°.
   b. Support the door to prevent it from falling.
   c. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge. See Figure 33 on page 55.
   d. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge. Pull the door out and towards you.
   e. Pull the door away from the chassis.
5. Remove the two 10-32 x 5/8 in. Phillips panhead screws with washers on each side. See Figure 41 on page 63 for the location of the screws.

6. If you are replacing the lower 2109 M12, go to step 7. If you are replacing the upper 2109 M12, go to step 8.
7. Install the bridge tool by completing the following steps:
   a. Remove the bridge tool from its box and adjust the two supports 45°.
   b. Hold the bridge tool between the two vertical supports near EIA unit 3.
   c. Move the two supports another 45°. Make sure that the following conditions are met:
      - The two-pin section of the support is on the back of the vertical support
      - The one-pin section of the support is on the front of the vertical support
   d. Align the two-pin section of the support on the back of the vertical rail with the bottom and middle holes in EIA unit 3.
   e. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 1.

      Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and one-pin sections with the vertical support.

   f. Lock the shelf into position.
8. For the upper 2109 Model M12, install the bridge tool by completing the following steps:
   a. Remove the bridge tool from its box and adjust the two supports 45°.
   b. Hold the bridge tool between the two vertical supports near EIA unit 20.
   c. Move the two supports another 45°. Make sure that the following conditions are met:
      - The two-pin section of the support is on the back of the vertical support
      - The one-pin section of the support is on the front of the vertical support
   d. Align the two-pin section of the support on the back of the vertical rail with the bottom and middle holes in EIA unit 20.
   e. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 18.
   f. Lock the shelf into position.
9. Locate the anti-tip bars and if they are not attached, attach them to the lift tool. If anti-tip bars were previously attached, go to step 10.
   a. Pull up on the leg-lock pins and insert the anti-tip bars inside the legs.
   b. Pull on the legs and anti-tip bars to ensure that they are locked into position.
   c. Raise the platform to allow enough room to attach the anti-tip bracket.
   d. Secure the anti-tip bars with the anti-tip bracket and bolt.
10. Move the lift tool to a position near the rear of the cabinet.
11. Turn the winch crank clockwise to raise the switch. Move the lift tool into position in front of the cabinet while you align the 24-inch load plate with the line on the bridge tool.
12. Turn the winch crank counterclockwise 1/4 turn to set the winch brake.
13. Set the wheel brake. Place the wheel chocks around the wheels.

ECT 10420 Paula

DANGER

A fully populated 2109 Model M12 weighs approximately 115 kg (250 lbs) and requires a minimum of two people and a lift tool to install it. Before you install it, verify that the additional weight of the chassis does not exceed the cabinet's weight limits or unbalance the cabinet. When you calculate the additional weight, include the cards or power supplies that partially extend out of the chassis.

CAUTION:
A pinch point exists between the 24-inch load plate and the bridge tool.

14. Slide the switch from the cabinet onto the 24-inch load plate. Center the switch on the platform.
15. Install the retention straps.
16. Remove the wheel chocks, release the wheel brake, and move the lift tool away from the cabinet.
17. Lower the load platform to its lowest position.
18. Remove the bridge tool.

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 111
Doc. 3698

10939 Paula

Chapter 7. Servicing the 2109 Model C36 with Model M12

This chapter contains information about how to power on and off the cabinet, and remove and replace FRUs and other system components.

Safety notices

The following safety notices apply to all the procedures in this chapter. Review this section carefully before you perform any power-related operations.

DANGER

An incorrectly wired electrical outlet could place hazardous voltage on metal parts of the system or the devices that attach to the system. The customer is responsible to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

Before you install or remove signal cables, ensure that you have unplugged the power cables for the system unit and all attached devices.

When you add or remove any additional devices to or from the system, ensure that you unplugged the power cables for those devices before you connect the signal cables. If possible, disconnect all power cables from the existing system before you add a device.

Use one hand, when possible, to connect or disconnect signal cables to prevent a possible shock from touching two surfaces with different electrical potentials.

During an electrical storm, do not connect cables for display stations, printers, telephones, or station protectors for communication lines.

CAUTION:
This unit might have more than one power cable. To completely remove power, you must disconnect all power cables from the unit.

CAUTION:
"Norway only:" This product is designed for an IT power system with phase-to-phase voltage of 230V. After operation of the protective device, the equipment is still under voltage if it is connected to an IT power system.

Power-on procedure

Perform the following steps to power on the cabinet:

1. Plug all power cords into the outlets on the power distribution units (PDUs).
2. Plug the power cord of each PDU into the customer's ac power outlets.

   CAUTION:
   This product is equipped with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded electrical outlet to avoid electrical shock.
3. Follow the power-on procedures for the 2109 Model M12 that is installed in the cabinet. See "Turning on and off the 2109 Model M12" on page 27.
4. Close the front door of the cabinet.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
69
Fls Nº
Doc 3698

Power-off procedure

Perform the following steps to power off the cabinet:

1. Open the rear door of the cabinet.

   Check the power cabling from the 2109 Model M12 that is attached to the PDU that you are servicing. These switches have dual power cords and are plugged into PDUs with independent ac sources.
2. Removing power to a mounted 2109 Model M12 has an adverse affect on the customer's systems and networks if they are not properly prepared. Inform the customer before you power off the 2109 Model M12.

   Before you power off switches, make sure that the customer has removed, dismounted, or taken them offline from their systems.
3. Turn off the ac power switches (circuit breaker) to the 2109 Model M12 that are connected to the PDU that you are servicing.
4. Unplug the power cord from the customer's ac power outlet.
5. Unplug all power cords from the PDU that you are servicing.

Removing and replacing a 16-port card or filler panel

Use this procedure to remove and replace a 16-port card or filler panel. The 2109 Model M12 can continue to operate during this procedure. However, if you are removing a 16-port card, any cables that are connected to that 16-port card must be disconnected.

You can notify the 2109 Model M12 of a hot-swap request in two ways. You can either run the **slotPowerOff** and **slotPowerOn** commands, or click the ejector handles on the 16-port card.

Attention: Do not remove the 16-port card during diagnostic tests. Wait for the status LED to turn off in response to the hot-swap request before you remove a 16-port card.

Attention: Disassembling any part of a 16-port card or filler panel voids the part warranty and regulatory certifications.

Attention: To ensure correct cooling of the chassis and protection from dust, install a filler panel in any empty slots.

CAUTION:
No user-serviceable parts are inside the 16-port card or filler panel.

Time required

Approximately 10 minutes or less

Removing a 16-port card or filler panel

Attention: Wear a grounded ESD strap when handling a 16-port card. The chassis has a grounding connection above the power connectors. Hold the 16-port card by the edges of the metal pan (do not hold by ejectors).

Note: If you are replacing multiple cards, replace one card at a time. Before you replace a port card, determine if it is the entire card or the SFPs that are faulty.

Perform the following steps to remove a 16-port card:

1. Ensure that traffic is not flowing through the port card (port LEDs should be off) before you disconnect the cables.
2. Disconnect any cables and SFP transceivers from the port card.
3. Notify the switch of a hot-swap request by pushing in the yellow tab on each ejector and clicking the black handles slightly open. See Figure 44 on page 72.

   Note: You can also send hot-swap notification from the command line interface by using the **slotpoweroff** and **slotpoweron** commands. See the *Brocade Fabric OS Procedures Guide* for additional command line instructions.
4. Wait for the Power LED to turn off in response to the hot-swap request before you uninstall the port card.
5. Lever both ejectors open to approximately 45° and pull the port card out of the chassis.

   Note: If you inadvertently re-latch the ejectors before you remove the card, wait at least one second before you unlatch the ejectors again.
6. If you are not replacing the card by another port card, install a filler panel to ensure correct cooling of the chassis and protection from dust. For more information, see "Replacing a 16-port card or filler panel" on page 74.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc 3698

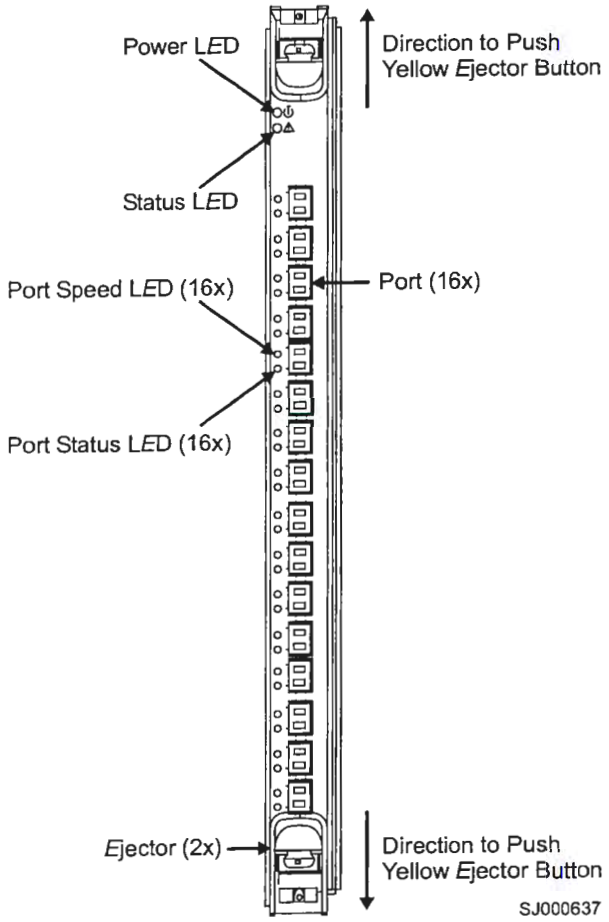


Figure 44. 16-port card showing ejectors

Removing a filler panel

The 2109 Model M12 accommodates the following two types of filler panels:

- A filler panel with ejectors
- A filler panel without ejectors

Perform the following steps to remove a filler panel with ejectors:

1. Push the yellow tab in on each ejector. See Figure 45 on page 73.
2. Lever both ejectors all the way open.
3. Slide the filler panel out of the chassis. See Figure 46 on page 74

Note: Filler panels without ejectors are equipped with a handle. Remove the two captive screws, grasp the handle, and slide the filler panel out.

10435
Paula

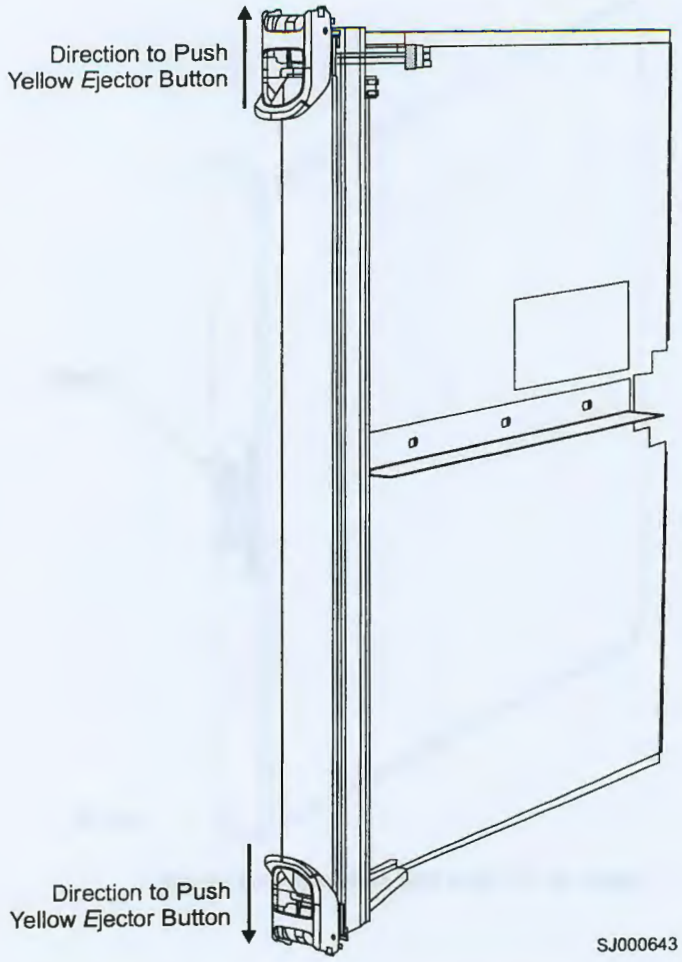


Figure 45. 16-port card filler panel

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1171
Doc - 3698

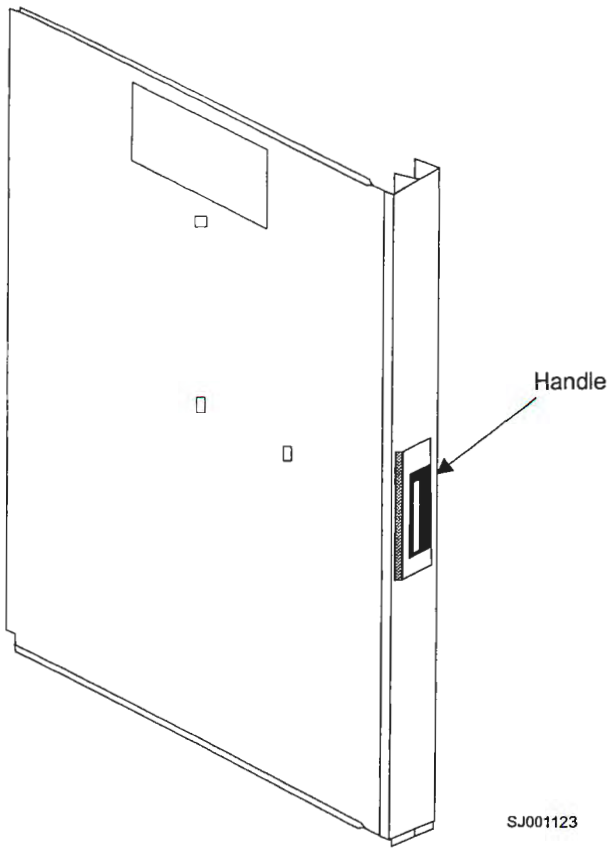


Figure 46. CP card filler panel with one handle

Replacing a 16-port card or filler panel

Attention: Do not force the installation. If the 16-port card or filler panel does not slide in easily, ensure that it is correctly aligned inside the rail guides before you continue.

Perform the following steps to replace a 16-port card or filler panel:

1. Orient the 16-port card or filler panel so that the ejectors are at the front of the chassis and the flat side of the 16-port card or filler panel is on the left.
2. Align the flat side of the 16-port card or filler panel inside the upper rail guides and the lower rail guides in the slot. See Figure 47 on page 75. Slide the 16-port card or filler panel into the slot, with slight pressure to the left, until it is firmly seated.
3. Close the ejectors by rotating the black handles toward the center of the 16-port card or filler panel until the ejectors lock. You will hear a slight audible click. The levering action of the handles seats the 16-port card or filler panel in the slot.

   Figure 47 on page 75 shows the alignment guides in the card slots.

ECT 10932 Paula

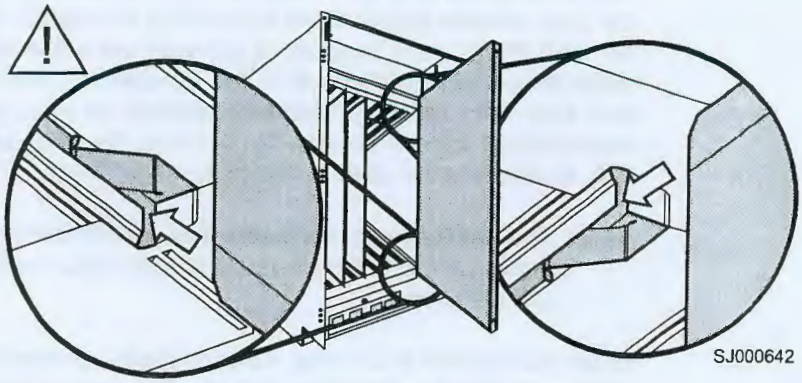


Figure 47. Alignment guides in the card slots

Perform these additional steps if you are installing a new 16-port card:

1. Verify that the power LED on the 16-port card is displaying a steady green light (it might require a few seconds to turn on). If it does not turn on, ensure that the 16-port card has power and is firmly seated. The front of the 16-port card should be flush with any adjacent 16-port cards or filler panels.

   Note: The LED patterns can temporarily change during a POST and other diagnostic tests.
2. Install SFPs and cables in the 16-port card, as required.
3. Group and route the cables as desired. See "Guidelines for managing cables" for more information.

   Attention: Do not route cables in front of the exhaust vent (located at the top of the chassis on the port side).

Guidelines for managing cables

The following guidelines are for managing cables:

- You can manage cables in a variety of ways. You can route them down through the cable management tray or route them out either side of the chassis. You can also manage them by using patch panels or cable channels on the sides of the cabinet.
- To keep the LEDs visible and to prevent having to disconnect the cables when removing neighboring cards, route fiber-optic cables and other cables directly downwards, instead of across adjacent cards or in front of the power supplies.
- Leave at least 1 m (3.28 ft) of slack for each fiber-optic cable, which:
  - Provides room to remove and replace the 16-port card
  - Allows for inadvertent movement of the cabinet
  - Prevents the cables from being bent to less than the minimum bend radius

  The minimum bend radius for a 50-micron cable is 3.05 cm (2 in.) under full tensile load and 3.048 cm (1.2 in.) with no tensile load.
- Use the cable guides that are provided with the 2109 Model M12 to group the cables by trunking ports (groups of four neighboring ports). These guides help to keep individual ports accessible by keeping the cables evenly spaced. They also help to provide clearance when removing a neighboring card.

Removing and replacing a CP card or filler panel

Use this procedure to remove and replace a CP card or filler panel.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
Doc. 3698

The 2109 Model M12 can continue to operate during this procedure if at least one CP card remains installed and functioning throughout the procedure. However, if the CP card that is being replaced is currently the active CP card, traffic over the fabric stops temporarily until failover to the standby CP card is complete. Failover takes less than 1 minute and occurs automatically as soon as the active CP card is uninstalled. If there is no standby CP card, the 2109 Model M12 stops functioning until at least one CP card is installed.

Note: The **haShow** command provides information about which CP card is the active CP card. For information about this command, see the *Brocade Fabric OS Reference*.

When you replace a CP card, it automatically assumes the native IP address and host name that is assigned to that slot. The default IP address and host name are `10.77.77.75 CP0`, for slot 5 and `10.77.77.74 CP1` for slot 6.

CAUTION:
Disassembling any part of a CP card or filler panel voids the part warranty and regulatory certifications. No user-serviceable parts are inside a CP card or filler panel. To ensure correct cooling of the chassis and protection from dust, install a filler panel in any slots that do not contain a CP card.

CAUTION:
Do not attempt to replace the RTC (real time clock) battery on the CP card. There is danger of explosion if you incorrectly replace the battery. Contact IBM because you must replace the battery with the same type of battery that the manufacturer recommends. You must also dispose of it according to the manufacturer's instructions.

Attention: Use the same version of Fabric OS on both CP cards and logical switches. Using different versions might cause malfunctioning. If the replacement CP card has a different version of the Fabric OS, bring both cards to the same firmware version.

Time required

30 minutes or less

Items required

- ESD grounding strap
- Workstation computer
- Serial cable provided with the 2109 Model M12
- IP address of an FTP server for backing up the switch configuration

Confirming a failed CP card

Before you replace the CP card, verify the necessity of the replacement. Any of the following events might indicate that a CP card is faulty:

- The Status LED on the CP card is orange, or the Power LED is not lit.
- The **slotshow** command does not show that the CP card is enabled.
- The CP card does not respond to commands or private Ethernet activities, or the serial console is not available.
- The **hashow** command indicates that the CP card has not achieved redundancy.

- The calendar clock is inaccurate, or the CP card does not start or shut down normally.
- Any of the following messages display in the error log:
  - Slot unknown message that relates to a CP slot
  - CP card errors
  - FRU: FRU_FAULTY messages for a CP card
  - Configuration loader messages or Sys PCI config messages
  - Generic system driver messages (FABSYS)
  - Platform system driver messages (Platform)
  - EM messages that indicate a problem with a CP card
  - Function fail messages for the CP master

For more information about diagnostic and error messages, see the *Brocade Diagnostic and System Error Message Reference* and the *Brocade Fabric OS Procedures Guide.*

Recording critical switch information for a CP card

Perform the following steps to record critical switch information:

1. Create a serial connection to the healthy CP card:
   a. Disable any serial communication programs that are running on the workstation (such as synchronization programs).
   b. Insert one of the serial cables into the terminal serial port. See the second port from the top in Figure 48 on page 80.
   c. Connect the other end of the serial cable to a serial port on the workstation. If necessary, you can remove the adapter on the serial cable to allow for a serial RJ45 connection.
   d. Open the terminal emulator application and configure as follows:
      - For most UNIX systems, type the following string at the prompt:
        `tip /dev/ttyb -9600`
      - For Windows 95, 98, 2000, or NT, see the following table for parameters and values.

Table 8. Parameters and values

Parameter	Value
Bits per second	9600
Databits	8
Parity	None
Stop bits	1
Flow control	None

   e. When the terminal emulator application stops reporting information, press Enter.
2. Log into the healthy CP card as `Admin`, then type `0` to log into switch 0. The default password is `password`.

See the following example for possible output.

```
Fabric OS (cp0)
cp0 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin>
```

3. Run the **haShow** command to determine which CP card is active. Do this from the serial console for the healthy CP card to verify the failover.

   Note: Enter all the remaining commands from the serial console for the active CP card, unless otherwise indicated.

4. If the healthy CP card is performing as the active CP card, go to step 7. If the faulty CP card is performing as the active CP card, fail over the cards as steps 4a through 4e describe:
   a. Create a serial connection to the faulty CP card (repeat step 1 on page 77.
   b. Log into the serial console as `Admin` and type `0` to log into logical switch 0.
   c. Run the **hafailover** command. The healthy CP card becomes the active CP card.
   d. Wait until the Status LED on the healthy CP card is no longer lit, which indicates that failover is complete.
   e. Run the **hashow** command from the serial console for the healthy CP card to verify the failover.

      See the following example for possible output.

```
Fabric OS (cp1)
cp1 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin> hashow
Local CP (Slot 6, CP1) : Active
Remote CP (Slot 5, CP0) : Standby
HA Enabled, Heartbeat Up
SW0:admin>
SW0:admin> hafailover
Warning: This command is being run on a control processor(CP)
based system and will cause the active CP to reset. This will
cause disruption to devices attached to both switch 0 and switch 1
and will require that existing telnet sessions be restarted.
To just reboot a logical switch on this system, use command
switchreboot(1M) on the logical switch you intend to reboot.
Are you sure you want to reboot the active CP [y/n]? y
SW0:admin>
SW0:admin> hashow
Local CP (Slot 6, CP1) : Standby, Healthy
Remote CP (Slot 5, CP0) : Active
HA Enabled, Heartbeat Up
SW0:admin>
```

5. Run the **version** command to record the version of the active CP card.
6. Run the **hadisable** command from the active CP card to prevent failover or communication between the CP cards during the replacement.
7. From the serial console for the healthy (and active) CP card, back up the current configuration for logical switch 0. See the possible output from the **configupload** command in step 8 on page 79.

10928 Paula

a. Run the **configupload** command.
b. Enter the requested information at the prompts.

8. Log into logical switch 1 and back up the current configuration for switch 1.
   a. From the serial console for the healthy CP card, enter the **login** command.
   b. Log into the switch as `Admin` and enter `1` to log into Switch 1.
   c. Enter the **configupload** command.
   d. Enter the requested information at the prompts.
      See the following example for possible output.

```
SW0:admin> configupload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
upload complete
SW0:admin>
SW0:admin> login
cp0 login: admin
Password: xxxxxx
Enter Switch Number to Login <0 or 1>: 1
SW1:admin>
SW1:admin> configupload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
upload complete
SW1:admin>
```

Removing a CP card or filler panel

Attention: Wear an ESD grounding strap when handling a CP card. The chassis has a grounding connection above the power connectors.

Attention: Hold the CP card by the edges of the metal pan (not by the ejectors).

Note: To allow the current configuration to be copied to the new CP card, you must install a new CP card while the other CP card is still operating.

Perform the following steps to remove a CP card:

1. Ensure that the other CP card is healthy and functioning as the active CP. See "Confirming a failed CP card" on page 76 for more information. Run the **haShow** command to determine which is the active CP card.
2. If the card that you are replacing is the standby CP card, continue with step 3. If the card that is being replaced is the active CP card, verify that the standby CP card is healthy. The power LED should be green, and the status LED should not be lit. Run the **haFailover** command to make the standby CP card act as the new active CP card.
3. Remove the CP card that you are replacing.
   a. Disconnect the following cables if they are present:
      - Modem cable from the modem serial port
      - Serial cable from the terminal serial port
      - Ethernet cable from the Ethernet port

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1117
Doc. 3698

b. Notify the switch of a hot-swap request by pushing the yellow tab on each ejector and clicking the black handles until they are slightly open. See Figure 48. Wait for the status LED to turn off.

   Attention: If you are removing a CP card, wait for the status LED to turn off in response to the hot-swap request before you uninstall the card.

c. Lever both ejectors all the way open, and slide the CP card out of the chassis.

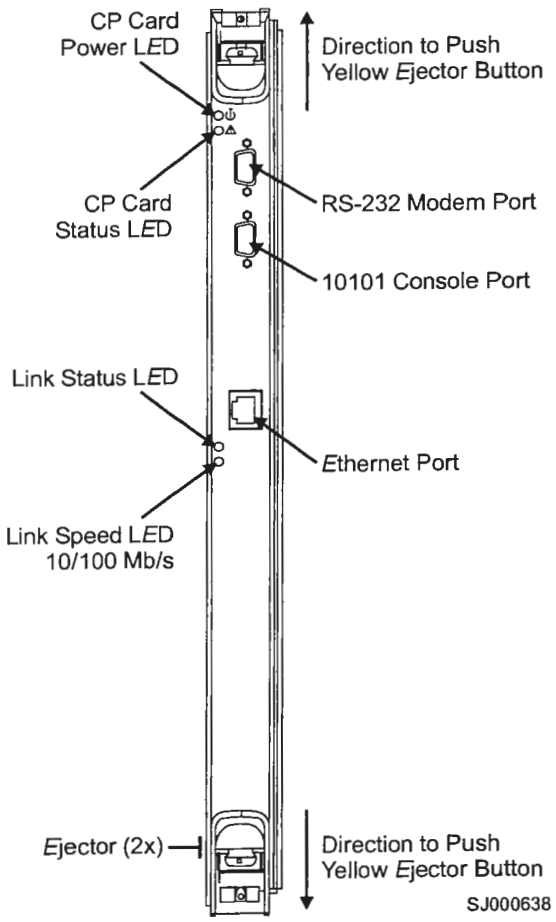


Figure 48. CP card showing ejectors

Perform the following steps to remove a filler panel:

1. Push in the yellow tab on each ejector. See Figure 49 on page 81.
2. Lever both ejectors all the way open.
3. Slide the filler panel out of the chassis.

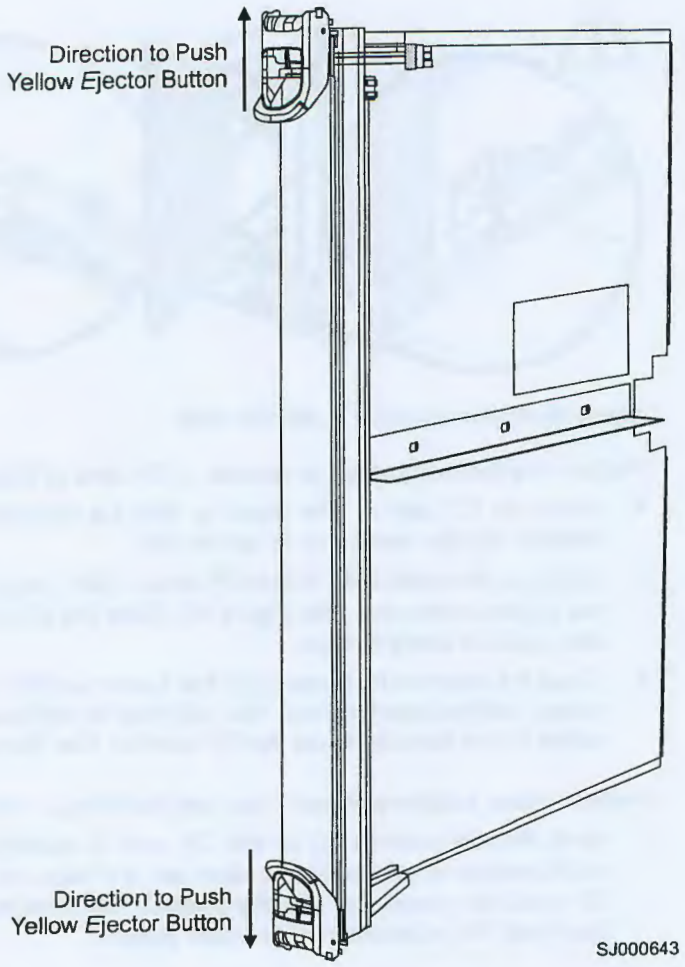


Figure 49. CP card filler panel with two ejectors

Replacing a CP card or filler panel

Attention: Do not force the installation. If the CP card or filler panel does not slide in easily, ensure that it is correctly oriented and aligned in the rail guides before you continue.

Figure 50 on page 82 shows the alignment guides in the card slots.

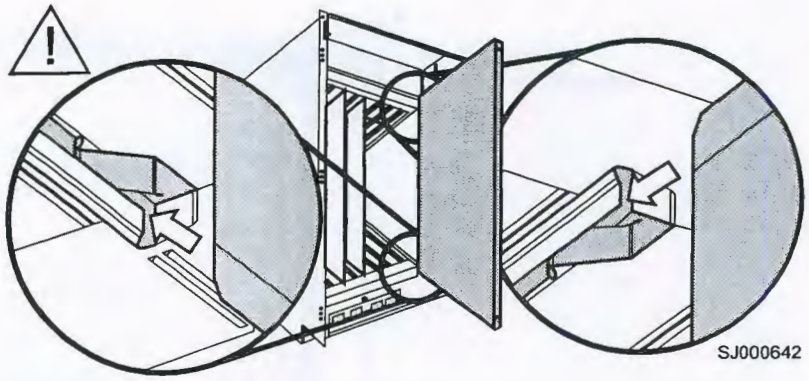


Figure 50. Alignment guides in the card slots

Perform the following steps to replace a CP card or filler panel:

1. Orient the CP card or filler panel so that the ejectors are at the front of the chassis and the metal pan is on the left.
2. Align the flat-metal side of the CP card or filler panel inside the upper and lower rail guides in the slot. See Figure 50. Slide the CP card or filler panel into the slot until it is firmly seated.
3. Close the ejectors by pressing in the black handles toward the CP card or filler panel, until the ejectors lock. You will hear a slight audible click. The levering action of the handles seats the CP card or filler panel in the chassis.

Perform these additional steps if you are installing a new CP card:

1. Verify that the power LED on the CP card is displaying a steady green light. It might require a few seconds to turn on. If it does not turn on, ensure that the CP card has power and is firmly seated. The front of the CP card should be flush with the adjacent cards or filler panels.

   Note: The LED patterns can temporarily change during a POST and other diagnostic tests.
2. Connect the cables as required to the CP card:

   Attention: Do not route the cables in front of the exhaust vent (located at the top of the port side of the chassis).
   - Modem cable to the modem serial port
   - Serial cable to the terminal serial port
   - Ethernet cable to the Ethernet port

Verifying the operation of the new CP card

Perform the following steps to verify that the new CP card is operational:

1. Verify that startup and POST are complete on the new CP card (a minimum of 3 minutes), and that the CP cards have achieved failover redundancy.
   a. Wait until the Status LEDs on both CP cards are not lit.

      If Fabric OS v4.0.2 or later firmware is installed on both CP cards, the Status LED for the active CP card displays orange until the active CP card is fully operational. The Status LED for the standby CP card displays orange until the CP cards have achieved failover redundancy.
   b. From the serial console for the active CP card (the CP card that was not replaced), run the **hashow** command and verify that the command output includes `HA Enabled Heartbeat Up`.

10924 Paula

The message HA-state in sync also displays. If not, POST is not complete or the CP cards have not yet achieved redundancy. Wait a minute and re-run the command until you can verify that redundancy has been achieved. See the sample output from the **hashow** command before redundancy is achieved.

```
SW1:admin> haShow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State not in sync
SW1:admin>
```

2. Run the **slotshow** command. The command output should show the new CP card as enabled, as the following output shows.

```
SW1:admin> slotShow
Slot Blade Type ID Status
--------------------------------
1 SW BLADE 2 ENABLED
2 SW BLADE 2 ENABLED
3 SW BLADE 2 ENABLED
4 SW BLADE 2 ENABLED
5 CP BLADE 1 ENABLED
6 CP BLADE 1 ENABLED
7 SW BLADE 2 ENABLED
8 SW BLADE 2 ENABLED
9 SW BLADE 2 ENABLED
10 SW BLADE 2 ENABLED
SW1:admin>
```

3. Determine the firmware version. For Fabric OS v4.0 and earlier, run the **version** command. For Fabric OS v4.0c and later firmware, run the **firmwareshow** command. Sample output for the **version** command and the **firmwareshow** command follows.

```
SW1:admin> version
Kernel: 2.4.2
Fabric OS: v4.0.0
Made on: Fri Feb 1 23:02:08 2002
Flash: Fri Feb 1 18:03:35 2002
BootProm: 3.1.13b
SW1:admin>

SW1:admin> firmwareshow
Local CP (Slot 5, CP0): Active
Primary partition: v4.0.2
Secondary Partition: v4.0.2
Remote CP (Slot 6, CP1): Standby
Primary partition: v4.0.2
Secondary Partition: v4.0.2
SW1:admin>
```

4. If the firmware versions on the replacement card do not match the active CP card, bring the replacement card to the same firmware level as the active card.
   a. Download the firmware by using either of the following command options:
      - Run the **firmwaredownload** command to download the firmware to both CP cards at the same time. Enter all requested information and choose the reboot option. If the switch is running Fabric OS v4.0.2 and later

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1
3698
Doc.

firmware, a message displays that warns you that this command causes the active CP card to reset. If this message displays, type Y to continue.

- If the firmware version of the replacement card is v4.1 or earlier, run the **firmwaredownload -s** command to download the firmware to only one of the CP cards. Enter all requested information and choose the reboot option. See the following sample output for the **firmwaredownload** command.

```
SW1:admin> firmwaredownload
Server Name or IP Address: 123.456.78.90
User Name: user
File Name: /v4.0.2/release.plist
Password: xxxxxx
Full Install (Otherwise upgrade only) [Y]:
Do Auto-Commit after Reboot [Y]:
Reboot system after download [N]: y
Start to install packages......
dir ################################################
terminfo ############################################
...
glibc ###############################################
sin #################################################
Write kernel image into flash.
file verification SUCCEEDED
Firmwaredownload completes successfully.
SW1:admin>
```

5. Verify that the restart is complete and that the CP cards have achieved failover redundancy.
   a. Wait until the Status LEDs on both CP cards are not lit.
   b. Run the **hashow** command and verify that the command output includes `HA Enabled Heartbeat Up`. If not, wait a minute and then rerun the command until you can verify that redundancy is achieved.
6. Run the **version** or **firmwareshow** command to verify that the firmware version has been updated.
7. Create a serial connection to the new CP card, as shown in step 1 on page 82.
8. Log into the new CP card as `Admin` and type `0` to log into logical switch 0. See the following sample output.

```
Fabric OS (cp1)
cp1 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin>
```

9. From the serial console for the new CP card, run the **hafailover** command to fail the active CP card over to the new CP card.
10. Verify that the configuration has successfully propagated to the new CP card by checking any configuration parameters for which you have specified non-default values. To do this, run the **configshow** command, followed by a text string (in quotation marks) that relates to the parameter, for example, **configshow "fabric"**. This limits the command output to entries that contain that text string.

10922 Paulo

Note: If you run the **configshow** command without a filter, it prints out approximately 1000 lines. For more information, see the *Brocade Fabric OS Reference.*

See the following sample output for the **configshow** command with the **"fabric"** as a filter.

```
SW0:admin> configshow "fabric"
fabric.domain:5
fabric.ops.BBCredit:16
fabric.ops.E_D_TOV:2000
fabric.ops.R_A_TOV:10000
fabric.ops.dataFieldSize:2112
fabric.ops.mode.fcpProbeDisable:0
fabric.ops.mode.isolate:0
fabric.ops.mode.longDistance:0
fabric.ops.mode.noClassF:0
fabric.ops.mode.tachyonCompat:0
fabric.ops.mode.unicastOnly:0
fabric.ops.mode.useCsCtl:0
fabric.ops.mode.vcEncode:0
...
SW0:admin>
```

11. Run the **haenable** command.
12. If the switch configuration does not replicate correctly, download the switch configurations that were backed up in step 8 on page 79.
    a. Run the **switchdisable** command to disable the current logical switch, which should still be switch 1.
    b. Run the **configdownload** command and enter the requested information.

       Note: If the switch is running Fabric OS v4.0.2, a message displays that cautions you about downloading the correct configuration file. If this message displays, type `Y` to continue.

    c. After the configuration is downloaded, run the **switchenable** command.
    d. Log into switch 0 and repeat steps 12a through 12c. See the following sample output for downloading the configuration to both logical switches.

RQS nº 03/2005 - CN CPMI - CORREIOS Fls Nº 1180 Doc. 3698

```
SW0:admin> switchdisable
SW0:admin> configdownload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
Committing configuration...done.
download complete
SW0:admin>
SW0:admin> switchenable
10 9 8 7 6 5 4 3 2 1
fabric: Principal switch
fabric: Domain 1
SW0:admin> login
cpl login: admin
Password:
Enter Switch Number to Login <0 or 1>: 1
SW1:admin>
SW1:admin> switchdisable
SW1:admin> configdownload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
Committing configuration...done.
download complete
SW1:admin> switchenable
10 9 8 7 6 5 4 3 2 1
fabric: Principal switch
fabric: Domain 1
SW1:admin>
```

13. Pack the old CP card in the packaging that is provided with the new card. Return the old CP card by using your local return policy.

Replacing the CP card battery

Each CP card has a lithium carbon-monoflouride coin cell battery that has a 10-year life expectancy. If the real-time clock (RTC) loses time, you might need to replace the battery. Contact IBM if the RTC begins to lose time.

CAUTION:
Replace only with the same or equivalent type of battery that the manufacturer recommends. Discard used batteries according to the manufacturer's instructions.

Removing and replacing a power supply or filler panel

Use this procedure to remove and replace a power supply. The 2109 Model M12 can continue to operate during the replacement if at least one power supply continues operating for every four 16-port cards that are installed. You need a minimum of two power supplies.

Note: You do not need to notify the 2109 Model M12 of a hot-swap request before you remove a power supply. Power supply filler panels are not required to ensure correct air flow.

The left power connector provides power to the power supplies in slots 1 and 3. The right power connector provides power to the power supplies in slots 2 and 4. The power connectors and the power supply slots are color-coded to identify which power connectors provide power to which power supply slots. See Figure 15 on page 3 for the location of the power supplies.

Attention: To protect against ac failure, you need a minimum of one power supply in slot 1 or slot 3, and one power supply in slot 2 or slot 4. If only two power supplies are installed and they are both installed in slots corresponding to the same power cable, unplugging a single power cable will power down the entire chassis.

Attention: If adequate power is abruptly lost, such as through removal of a power supply, the entire switch is powered down. The power off order that the **powerOffListSet** command designates is not followed.

Attention: Disassembling any part of the power supply voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the power supply.

Time required

Less than 5 minutes

Removing a power supply or filler panel

Perform the following steps to remove a power supply or filler panel:

1. If the 2109 Model M12 is going to operate during the replacement procedure, check the LEDs to verify that the minimum of two power supplies are functioning before you uninstall the power supply.
2. Remove the power supply or filler panel from the chassis. See Figure 51 on page 88 for the location of the power supply.

10420 Paula
ROS nº 03/2005 - CN CPMI - CORREIOS
Fls Nº 1181
Doc. 3698

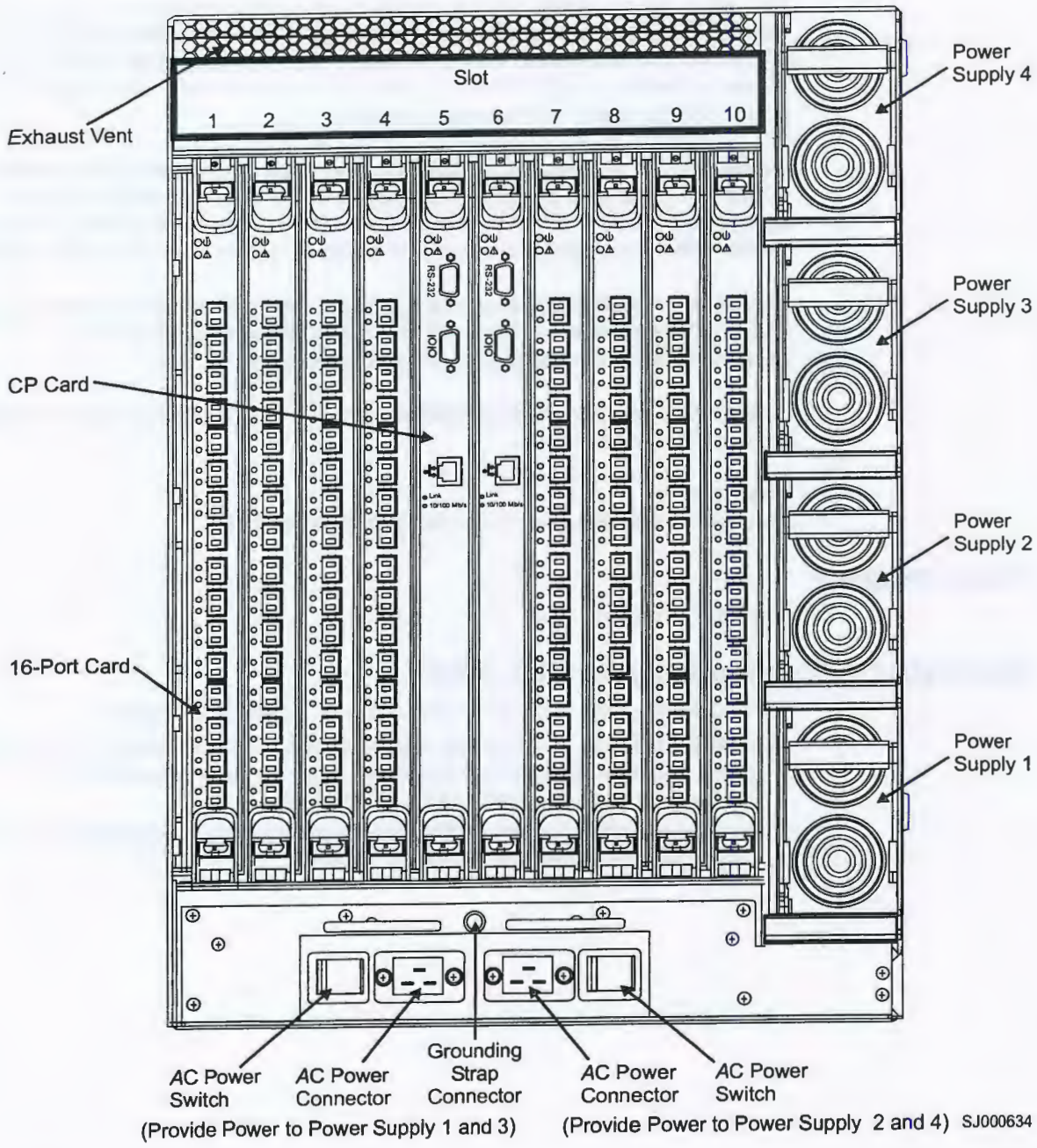


Figure 51. Location of the power supplies

Attention: Support the power supply from underneath while removing it from the chassis.

a. Remove the power supply by pushing the locking tab in towards the power supply then pull the handle out and down, and use the handle to pull the power supply out of the chassis. See Figure 52 on page 89.

b. Remove the filler panel by pulling it out by the handle.

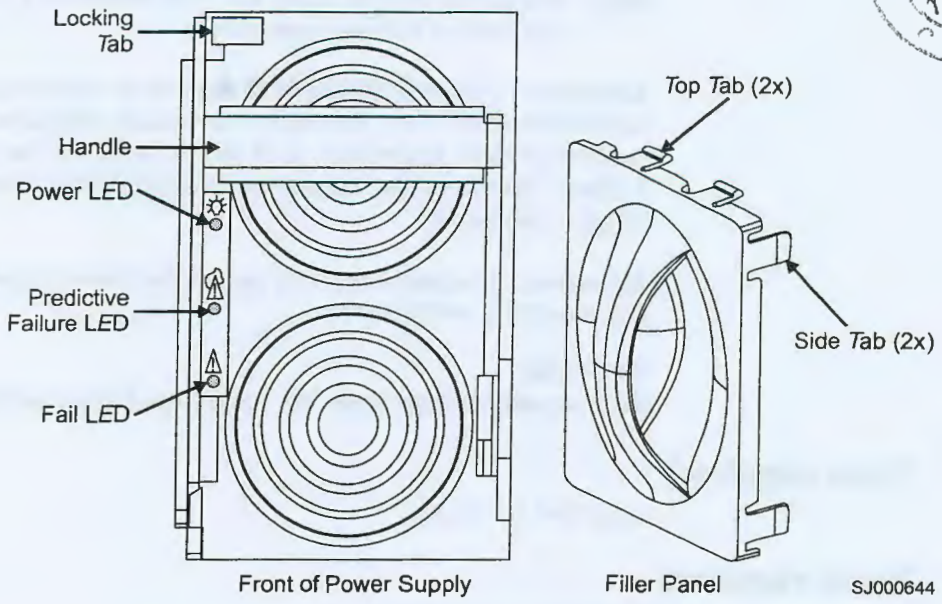


Figure 52. Power supply and filler panel

Replacing a power supply or filler panel

Attention: Do not force the installation of the power supply or filler panel. If the part does not install easily, ensure that it is properly oriented.

Perform the following steps to replace a power supply:

1. Orient the power supply so that the handle is toward the front of the chassis and the LEDs are on the left.
2. Unlock the handle and insert the power supply all the way into the slot.
3. Push the handle up until it clicks.
4. Verify that the power supply is seated by pulling gently on the handle.

Perform the following steps to replace a filler panel:

1. Orient the filler panel so that the handle is vertical and side tabs are on the right.
2. Push the filler panel into the slot.

Perform these additional steps if you are installing a new power supply:

1. Verify that the top LED on the power supply displays a steady green light.
2. If a green light is not displayed, ensure that both power cables are plugged in and that both ac switches are flipped to "|" (the ac switch lights up green).

Removing and replacing a blower assembly

Use this procedure to remove and replace the blower assembly. The 2109 Model M12 requires that a minimum of two of the three blower assemblies are operating. It can continue to operate during the replacement only if the other two blower assemblies continue to operate. If more than one blower must be turned off at the same time, you should turn off the 2109 Model M12 to prevent overheating.

Note: You do not need to notify the 2109 Model M12 of a hot-swap request before you remove a blower assembly.

Attention: The 2109 Model M12 requires a minimum of two operating blower assemblies at all times. To ensure continuous adequate cooling, maintain three operating blower assemblies at all times except for the brief period when replacing a blower assembly. The 16-port cards automatically shut down if the temperature range is exceeded.

Attention: Disassembling any part of the blower assembly voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the blower assembly.

Time required

Less than 5 minutes

Items required

#2 straight screwdriver

Removing a blower assembly

Perform the following steps to remove a blower assembly:

1. Before you remove the blower assembly, verify that the other two blower assemblies are functioning correctly. The blower assembly power LED should be steady green, and the fault LEDs should not be lit (see Figure 53 on page 91 for LED locations). For information about how to check the status of the blower assembly by using Telnet, see the *Brocade Fabric OS Reference*.
2. Remove the blower assembly from the chassis.

   CAUTION:
   Support the blower assembly from underneath while removing it from the chassis.

   a. Use the screwdriver to loosen the thumbscrews at the top and bottom of the blower assembly. See Figure 53 on page 91.
   b. Push in the top part of the handle. Pull out the lower part of the handle and pull the blower assembly out of the chassis.

Replacing a blower assembly

Attention: Do not force the installation. If the blower assembly does not slide in easily, ensure that it is properly oriented before you continue with the installation.

Perform the following steps to replace a blower assembly:

1. Orient the blower assembly. See Figure 53 on page 91.
2. Slide the blower assembly into the chassis, pushing firmly to ensure that it is seated.
3. Verify that the power LED displays a green light. If a green light is not displayed, ensure that the blower assembly is seated correctly.
4. Push the top of the handle into the recess.
5. Tighten the thumbscrews on the blower assembly to finger-tight.

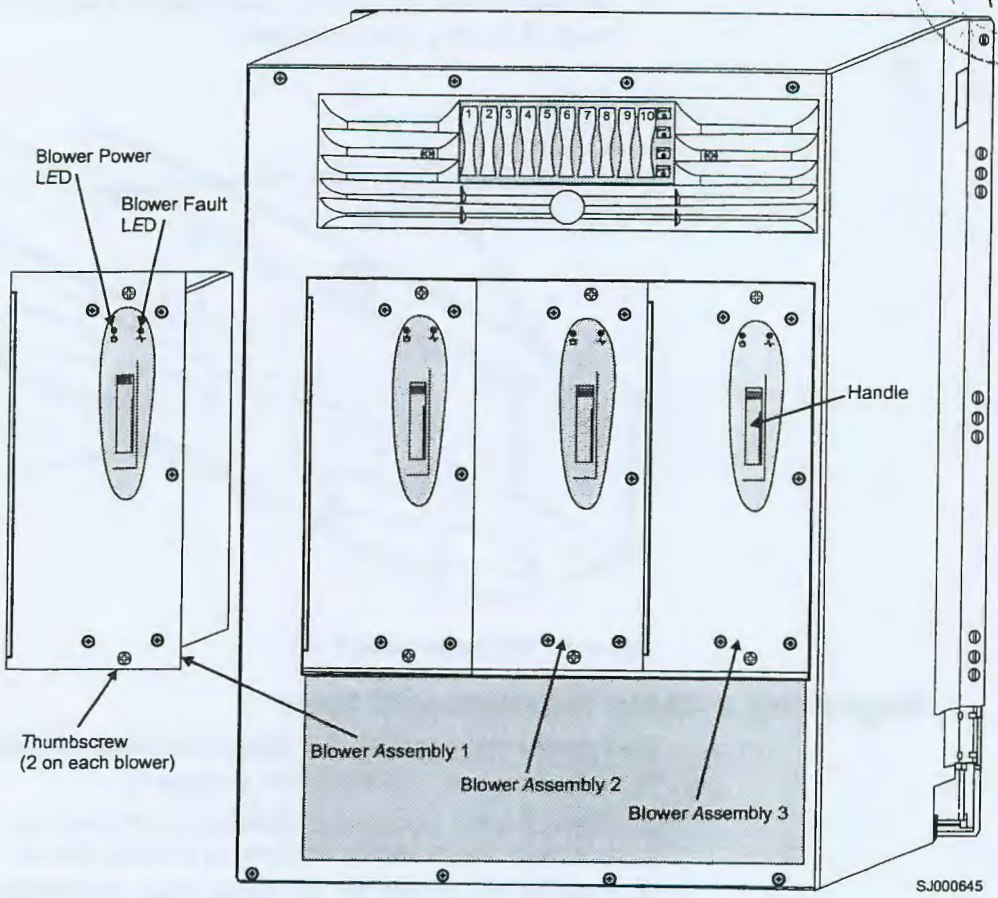


Figure 53. Blower assembly side of the 2109 Model M12 shown with one blower assembly uninstalled

Removing and replacing the cable management tray

Use this procedure to remove and replace the cable management tray. The 2109 Model M12 can continue to operate during the replacement.

Attention: Do not use a power screwdriver on the cable management tray.

Time required

Less than 5 minutes

Items required

#2 Phillips screwdriver

Removing a cable management tray

Perform the following steps to remove a cable management tray:

1. Pull any cables out of the cable management tray.
2. Unscrew the two screws that hold the tray to the chassis. See Figure 54 on page 92 for the location of the screws. Save the screws for reuse when you replace the cable management tray.

3. Rotate the front of the tray down, then lift the back to disengage the tabs on the back of the tray from the chassis.

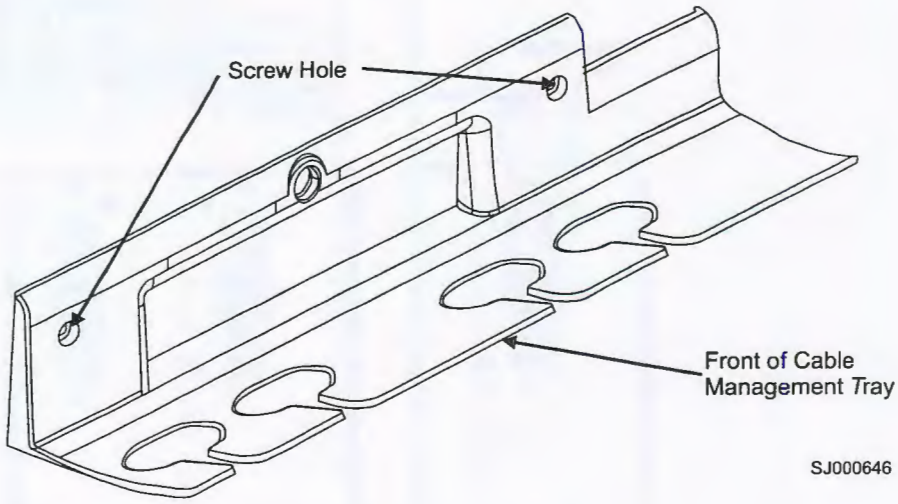


Figure 54. Cable management tray

Replacing a cable management tray

Perform the following steps to replace the cable management tray:

1. Orient the tray. See Figure 55 on page 93.
2. Insert the two tabs on the underside of the tray into the two slots at the bottom of the ac panel. Rotate the front of the tray up until it locks into place.
3. Position and tighten the two screws that you previously removed.
4. Arrange the cables through or along the tray as required.

Note: Route the power cables out each side of the chassis.

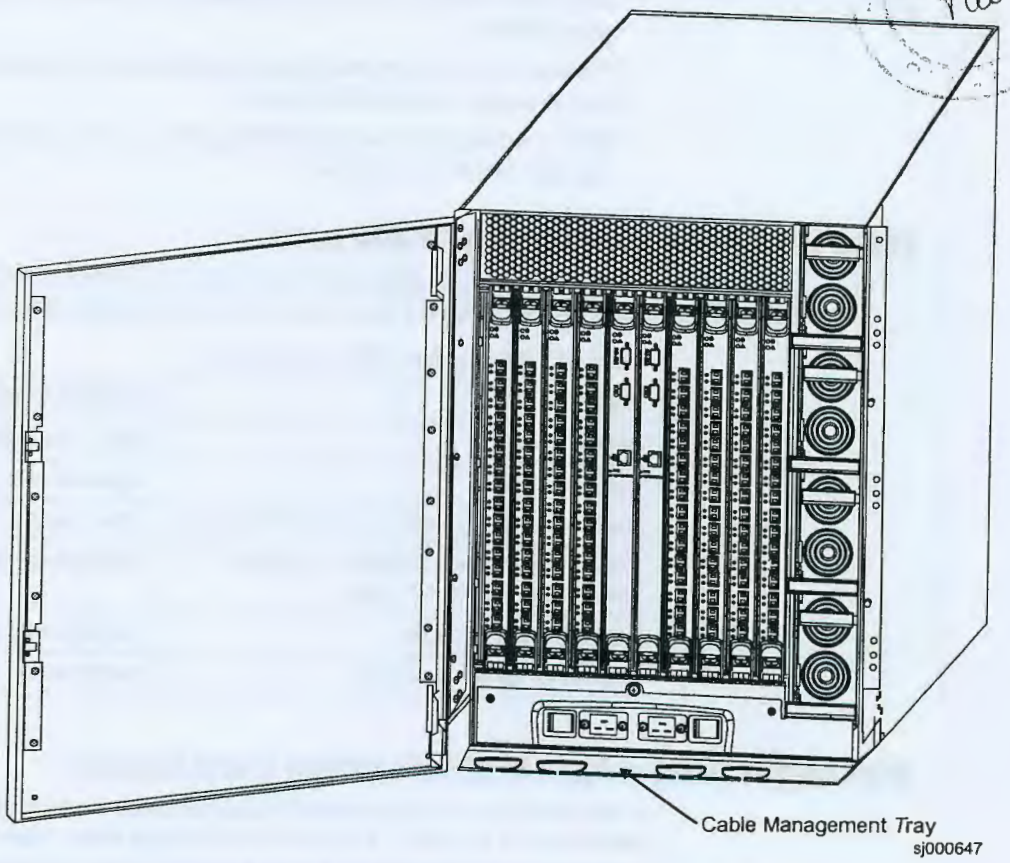


Figure 55. 2109 Model M12 with the cable management tray

Removing and replacing the WWN card

The WWN card is highly reliable. Before you replace the WWN card, verify that a replacement is necessary. If you are installing a new WWN card, the installation instructions are included with the product.

If you are going to replace a WWN card for Fabric OS earlier than v4.1.0, you must power down the 2109 Model M12. Do not remove the WWN card until you have received the replacement card. Do not restart the switch with a failed or missing WWN card.

Note: You must consult with Technical Support before you replace the WWN card.

Verifying if the WWN needs replacing

Ensure that the current card is firmly seated when you perform troubleshooting steps.

Note: You must consult with Technical Support before you replace the WWN card.

Any of the following events might indicate that the WWN card needs to be replaced:

- Visible mechanical damage to the WWN card

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1184
3698
Doc.

- Any of the Status LEDs on the WWN card do not reflect the actual status of the components
- Problems viewing or modifying the data that is stored on the WWN (see "Data that is stored on the WWN card")
- Error messages regarding WWN unit 1 or unit 2 (see Messages that might indicate WWN card failure)

Data that is stored on the WWN card

Table 9 shows the data that is stored on the WWN card. The WWN card might need to be replace if you have difficulty retrieving or modifying this data.

Table 9. Data that the WWN card stores

Data	Related Commands
WWN values	wwn, chassisshow
License keys	licenseshow, licenseadd, licenseremove
Data about the chassis and the WWN card	chassisshow
Ethernet and Fibre Channel IP address information for the CP cards	ipaddrshow, ipaddrset
History log information	historyshow, historylastshow
Names of logical switches	switchname

Messages that might indicate WWN card failure

If the error log or serial console display error messages that indicate problems with WWN unit 1 or unit 2, the WWN card might have failed. WWN unit 1 and unit 2 correspond to information that is specific to the WWN card, and are displayed by the **chassisshow** command. Table 10 shows messages that might indicate WWN card failure. For more information about error messages, see the *Brocade Diagnostics and System Error Message Reference*.

Note: WWN unit 1 and unit 2 do not correspond to the WWNs for logical switches 0 and 1.

Table 10. Sample error messages

Type of Message	Sample Error Message
WWN unit 1 or unit 2 fails its field replacable unit (FRU) header access	0x24c (fabos): Switch: 0, error EM-I2C_ TIMEOUT, 2, WWN 1 I2C timed out: state 0x4
WWN unit 1 or unit 2 is being faulted	0x24c (fabos): Switch: 0, Critical EM-WWN_ UNKNOWN, 1, Unknown WWN #2 is being faulted
WWN unit 1 or unit 2 is not present or is not accessible	0x24c (fabos): Switch: 0, Error EM-WWN_ ABSENT, 2, WWN #1 not present
Writing to the FRU history log (hilSetFruHistory) has failed	0x24c (fabos): Switch: 0, Error EM-HIL_FAIL, 2, HIL Error: hilSetFruHistory failed, rc=-3 for SLOT 3

Removing and replacing the PDU

Use this procedure to remove and replace the PDU. See Figure 57 on page 116 and Figure 58 on page 117 for the orientation of the PDU and the power cords.

Removing the PDU

Complete the following steps to remove the PDU from the cabinet:

1. Follow the steps in "Power-off procedure" on page 70.
2. Turn off power and disconnect the ac power distribution bus from the customer's ac power outlet. Record the locations of the switch ac power cables that are plugged into the PDUs.
3. Unplug the switch ac power cables from the PDUs.
4. Remove the four mounting screws from the PDU. Pull the unit toward you.
5. Remove the PDU from the cabinet.
6. Remove the four M6 screws from the dual device attachment bracket (the center bracket attaching the two PDUs together). Set the screws aside for reuse when you replace the PDU.
7. Remove the two M3 x 5 screws from the dual-device attachment bracket of the PDU that you are replacing. Set the screws aside for reuse when you replace the PDU.
8. Remove the two M3 x 5 screws from the horizontal mounting bracket of the PDU that you are replacing (the bracket that is attached to the cabinet). Set the screws aside for reuse when you replace the PDU.

Replacing the PDU

Complete the following steps to replace a PDU in the cabinet:

1. Replace the horizontal mounting bracket on the new PDU by using the two M3 x 5 screws that you removed during the removal procedure.
2. Replace the dual device attachment bracket by using the two M3 x 5 screws that you removed earlier in the procedure.

   Note: Make sure that the threaded holes are on the opposite side of the device as the holes on the other attachment bracket.
3. Push the two PDUs together, aligning the holes on the dual device attachment brackets.
4. Secure the front and rear of the brackets to each other by using the four M6 screws that you removed during the removal procedure.
5. Slide the PDU into position. Install the four mounting screws.
6. Reconnect any power cables that you disconnected from the PDU.
7. Plug the power cables into the locations that you recorded during the removal procedure.
8. Follow the steps in "Power-on procedure" on page 69.

Removing and replacing the chassis door

Use this procedure to remove and replace the chassis door on the 2109 Model M12.

Note: The chassis door is required to ensure that the 2109 Model M12 meets electromagnetic interference (EMI) and other regulatory certifications.

Time required

Less than 5 minutes

RQS nº 03/2005 - CN
Fls. Nº 1185
Doc. 3698

Removing the chassis door

Perform the following steps to remove the chassis door:

1. Open the door 90°.
2. Support the door to prevent it from falling.
3. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge.
4. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge. Pull the door out, towards you.
5. Pull the door away from the chassis.

Replacing the chassis door

Perform the following steps to replace the chassis door:

1. Ensure that the levers on the spring-loaded pins on both hinges are pushed into the notches.
2. Align the spring-loaded pins with the chassis portion of the hinges.
3. Release the pins by pushing the levers out of the notches.

Removing and replacing the front or rear cabinet door

Use this procedure to remove and replace the front or rear cabinet doors.

Removing the cabinet door

Perform the following steps to remove the front or rear door:

1. Open the door of the cabinet.
2. Remove the door by lifting it up and out.
3. Remove the hinge bracket (if necessary) by removing the hinge mounting screws that attach the bracket to the rack. See Figure 56.

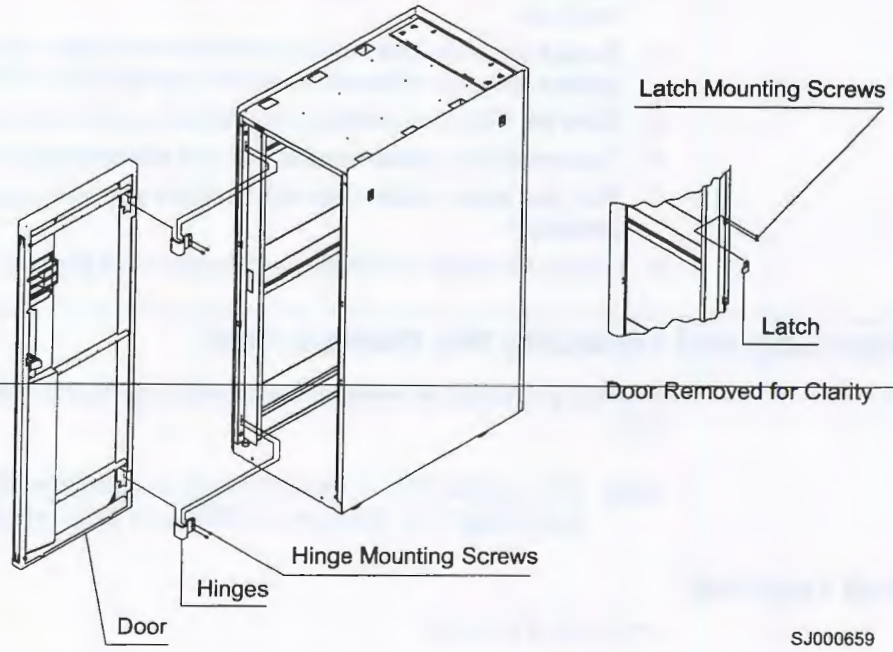


Figure 56. Removing the cabinet door

Replacing the cabinet door

Perform the following steps to replace the front or rear door:

1. Align the door with the hinge pin.
2. Install the bottom hinge pin (the longest pin) first.
3. Install the top hinge pin (the shortest pin) second.

Relocating the cabinet

Perform the following steps to relocate the cabinet:

1. Turn off all power to the cabinet and the 2109 Model 12 that is installed.
2. Disconnect all power and all device cables.
3. Unbolt the cabinet from the floor or remove the stabilizers.
4. Raise all the leveling feet.
5. Unlock each caster wheel by loosening the screw on the caster.
6. Move the cabinet to the new position.
7. Reposition the cabinet. Go to "Step 1. Position the cabinet" on page 7.

Reference information for the fruinfoset command

You must run the **fruinfoset** command through the active CP card by using root access. For more information, see Table 11.

Table 11. Reference information for the fruinfoset command

Name	fruinfoset
Syntax	`fruinfoset`
Availability	Factory or root only
Description	This command provides for the setting of the four externally modifiable fields in the header that is associated with each FRU. After the new data is written, the final contents of the fields are printed. No other fields can be modified. Some FRUs might not contain customer data or might not be programmable, in which case an error message displays.
Operands	**FRU ID** and **number** are the required operands. **FRU ID** Type of FRU: • Slot (port card or CP card in a slot) • Fan (blower assembly) • Ps (power supply) • Chassis (chassis or WWN card) **number** Physical slot or unit number for which the information will be input. For chassis information, type `chassis 1`. For WWN card information, type `chassis 2`.

RQS nº 03/2005 - CN
Fls Nº 1186
Doc. 3698

Table 11. Reference information for the fruinfoset command (continued)

Usage	The modifiable fields and their maximum field sizes are as follows: **Field name** **Maximum number of characters** ID 10 characters PN (part number) 20 characters SN (OEM serial number) 20 characters RV (revision code 4 characters Chassis SN (serial number) 12 characters (This field displays only when the chassis 1 parameter is used.) These fields might not display for all FRUs. For each field that displays, the existing value displays followed by a > prompt for the new value. If more than the allowed number of characters are entered, the extra characters at the end are ignored, and a warning message displays. Leading blanks are also ignored. The `chassis SN` prompt displays only if the chassis 1 parameter is entered after the command. The usage rules are the same as for other values. The chassis serial number is identified by the **chassisShow** command as the `Serial Num for Chassis/WWN: Unit 1`

Appendix A. Product specifications

This appendix contains the 2109 Model C36 with Model M12 specifications.

2109 Model M12 components

The 2109 Model M12 contains the following components:

- A 14U chassis, designed to be mounted in a 48.26 cm (19 in.) rack. Two 2109 Model M12 switches can be mounted in a 2109 Model C36 cabinet.
- 16-port cards in configurations up to eight cards per chassis, with 16 optical ports per card, compatible with SFPs.
- Two CP cards, each with:
  - One modem serial port with a DB-9 connector (full RS-232)
  - One terminal serial port with a DB-9 connector (RS-232 signal subset)
  - One IEEE compliant RJ-45 connector for use with a 10 Mbps or 100 Mbps Ethernet connection
  - A real-time clock (RTC) with a 10-year battery and 56 bytes of NVRAM
- Four power supplies with built-in fans. The power supplies plug into internal blind-mate connectors when installed in the chassis.
- Two ac power inlet connectors with ac power switches (power panel).
- A WWN card and bezel.
- Three blower assemblies for forced-air cooling of the 16-port cards and the CP cards.

Air enters inlet vents on the blower assembly side of the chassis and exits through vents on the port side of the chassis. The blower speed is governed by inlet air temperature. The blowers go into high speed when the inlet air temperature exceeds 33°C (91°F).

Physical dimensions

The dimensions of the 2109 Model M12 are listed in Table 12.

Table 12. Physical dimensions of the 2109 Model M12

Dimension	Value
Height	14U (24.11 in.)
Depth	70.9 cm (27.9 in.)
Depth with door	72.9 cm (28.7 in.)
Width	43.7 cm (17.2 in.)

2109 Model M12 and component weights

The weight of a fully loaded 2109 Model M12, as well as the weights of individual components, are listed in Table 13.

Table 13. Component weights

Component	Weight
Fully loaded chassis	Approximately 114 kg (250.0 lbs)
Empty chassis	47.1 kg (104.0 lbs)

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1187
Doc. 3698

Table 13. Component weights (continued)

Component	Weight
Door	3.4 kg (7.6 lbs)
Blower assembly	4 kg (8.8 lbs)
Power supply	3.2 kg (7.0 lbs)
WWN bezel	0.27 kg (0.6 lbs)
CP card	2.5 kg (5.6 lbs)
16-port card	3.9 kg (8.6 lbs)
Card filler panel	1.6 kg (3.2 lbs)
Cable management tray	0.27 kg (0.6 lbs)

2109 Model C36 with Model M12 specifications

The specifications for the 2109 Model C36 with Model M12 are listed in Table 14.

Table 14. 2109 Model C36 with Model M12 specifications

Dimension	Value
Height	1785 mm (70.3 in.)
Depth	• With rear door installed: 1042 mm (41 in.) • With rear and front door installed: 1098 mm (43.3 in.)
Width	• With side panels installed: 650 mm (25.6 in.) • Without side panel installed: 623 mm (24.5 in.)
EIA units	36 EIA units
Weight	Cabinet with two 2109 Model M12 switches: 816 kg (1795 lbs)

16-port card specifications

The ports in the 2109 Model C36 with Model M12 support full duplex link speeds at 2.125 Gbps or 1.0625 Gbps, inbound and outbound, automatically negotiating to the highest common speed of all the devices that are connected to the port. Each port has a serializer/deserializer (SERDES) which accepts 10-bit wide parallel data and serializes it into a high-speed serial stream. The parallel data is expected to be 8B/10B encoded data or equivalent.

The ports are compatible with optical SWL (780 - 850 nm), and optical LWL (1270 - 1350 nm), SFPs, and SFP-compatible cables. The strength of the signal is determined by the type of SFP that is being used.

The ports are universal and self-configuring, and are capable of becoming F_ports, FL_ports, or E_ports.

The ports meet all required safety standards. For more information about these standards, see Table 22 on page 106.

CP card specifications

This section describes the specifications for the CP card.

Memory specifications

The centralized memory maximizes switch throughput by guaranteeing full transmit and receive bandwidth to all Fibre Channel ports at all times.

Each CP card contains the type and specification of memory listed in Table 15.

Table 15. Memory specifications

Memory type	Amount
Main memory	256 MB of SDRAM (32 bits wide)
Flash memory	• User flash: 16 MB of 16-bit wide memory, stored in two 8 MB banks • Compact flash: 256 MB, partitioned in two 128 MB sections
Boot flash memory	512 KB of 8-bit wide memory for system startup

Battery specifications

The CP card has a lithium carbon-monoflouride coin cell battery.

Table 16 lists the battery specifications.

Table 16. Battery specifications

Type	Specification
Rayovac BR1225	3.0 volt, 50 mAh

CAUTION:
There is danger of explosion if the battery is incorrectly replaced. All used batteries must be discarded according to the manufacturer's instructions. Contact IBM if the real time clock begins to lose time.

Terminal serial port specifications

Each CP card provides a terminal serial port with a DB-9 connector with an RS-232 signal subset.

Note: For dust and ESD protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

The terminal serial port is intended primarily for use during the initial setting of the IP address and for service purposes.

A 3.0m (10 ft) serial cable is provided with the switch. You can convert it from a DB-9 serial cable to an RJ-45 style serial cable by removing the adapter on the end of the cable.

You can use the terminal serial port to connect to a computer workstation or terminal without connecting to the fabric. The terminal device should be configured to 9600 baud, 8 data bits, no parity, 1 stop bit, with no flow control.

The terminal serial port requires a straight through serial cable with a female 9-pin D-SUB connector. Use the pinouts listed in Table 17 on page 102.

10306 Fauke
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1188
3698
Doc.

Table 17. Pinouts with signal and description

Pin	Signal	Description
1		
2	TxData	Transmit data
3	RxData	Receive data
4		
5	GND	Logic ground
6		
7		
8		
9		

Modem serial port specifications

Each CP card has a modem serial port (labeled RS-232) with a fully RS-232 compliant DB-9 connector.

Note: For dust and ESD protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

You can use the modem serial port to attach a modem to each CP card. The 2109 Model M12 detects modems only during the power-on or restart sequences, and automatically initializes them for operation. If modems are connected to an operating switch, a power on and off cycle, restart, or fast restart is required in order to detect the modems.

Customers should connect a "Y" cable on the telephone line to each modem. The active CP card answers on the first ring. The standby CP card answers on the seventh ring if the active CP card has failed to answer.

The modem serial port pinouts are listed in Table 18.

Table 18. Modem serial port pinouts

Pin	Signal	Description
1	DCD	Data carrier detect
2	RxData	Receive data
3	TxData	Transmit data
4	DTR	Data term ready
5	GND	Logic ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

Fibre Channel port specifications

The Fibre Channel ports in the Model M12 support full duplex link speeds at 2.125 Gbps or 1.0625 Gbps inbound and outbound. The ports automatically negotiate to the highest common speed of all devices that are connected to the port. Each port

has a SERDES that accepts 10-bit wide parallel data and serializes it into a high-speed serial stream. The parallel data is expected to be 8B/10B encoded data or equivalent.

The ports are compatible with the following SFPs and SFP-compatible cables:

- Optical SWL: 780 - 850 nm
- Optical LWL: 1270 - 1350 nm

The strength of the signal is determined by the type of SFP in use.

The ports are universal and self-configuring, and are capable of becoming F_ports, FL_ports, or E_ports. These ports meet all the required safety standards.

Facility specifications

To ensure correct operation of the 2109 Model C36 with Model M12 , ensure that the facility meets the following specifications:

- Power requirements for a physical inlet:
  - Input power requirements: 200 - 240 V ac, 24A, 50 - 60 Hz
  - Recommended power connector
- An adequate supply circuit, line fusing, and wire size, according to the electrical rating on the switch nameplate.
- An air flow of at least 350 cubic feet per minute per switch, available in the immediate vicinity of the 2109 Model C36 with Model M12.
- The power specifications listed in "Power specifications".
- The environmental specifications listed in "Environmental requirements" on page 104.
- Interference less than the standard levels listed in Table 21 on page 105, under Immunity.

Power specifications

CAUTION:
To remove power to the 2109 Model M12, disconnect both power cables.

The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections and distributed name server (DNS). It is electro-magnetic compatibility (EMC) compliant.

The power supplies are universal and capable of functioning worldwide without using voltage jumpers or switches. They meet IEC 61000-4-5 surge voltage requirements and are autoranging in terms of accommodating input voltages and line frequencies. Each power supply has its own built-in fan for cooling. The fans push the air towards the port side of the chassis.

The power specifications listed in Table 19 on page 104 are calculated for fully-loaded systems with four power supplies. A fully-loaded system has eight 16-port cards, two CP cards, and three blower assemblies.

Table 19 on page 104 lists the power specifications for the 2109 Model C36 with Model M12.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1189
Doc. 3698

Table 19. Power specifications

Specification	Value
Total power available from each power supply	1 KW
Input voltage	200 - 240 V ac
Input line frequency	50 - 60 Hz
Harmonic distortion	Active power factor correction per IEC1000-3-2
Heat output (BTU rating)	• 64 ports: 1080 Watts, 3690 BTU per hour • 128 ports : 1960 Watts, 6700 BTU per hour
Maximum inrush current per power cord	40 amps peak
Input line protection	Thermal circuit breaker
Power supply dimensions	6.96 cm (2.74 in.) wide, 12.34 cm (4.86 in.) high, 34.29 cm (13.50 in.) long

Environmental requirements

Table 20 lists the environmental operating ranges for the 2109 Model C36 with Model M12. The requirements for non-operating conditions are also provided for acceptable storage and transportation environments.

Table 20. Environmental requirements

Condition	Acceptable range during operation	Acceptable range during nonoperation
Temperature (See Note)	0° - 40°C (40° - 104°F)	0° - 40°C (40° - 104°F)
Humidity	20% - 80% RH noncondensing, at 40°C	0% - 90% RH noncondensing, at 40°C
Altitude	0 - 3 km (0 - 10 000 ft) above sea level	0 - 12 km (0 - 39 370 ft) above sea level
Shock	4G, 11 MS duration, half-sine wave	0G, 11 MS duration, sq wave
Vibration	5G, 0 - 3 kHz at 1.0 octave per minute	10G, 0 - 5 kHz at 1.0 octave per minute
Heat dissipation	• 64 ports: 3690 BTU per hour • 128 ports: 6700 BTU per hour	Not applicable
Note: Temperature measured at the air inlets on the blower assembly side of the chassis.		

General specifications

Table 21 lists the general specifications for the 2109 Model C36 with Model M12.

Table 21. General specifications

Specification	Description
Configurable port types	The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections.
EMI rating	An operating 2109 Model C36 with Model M12 conforms to the EMI radiation levels specified by the following regulations: • FCC Rules and Regulations, Part 15B, Class A level • CISPR22 Class A • EN55022 Class A • VCCI Class A ITE • AS/NZS 3548 Class A • CNS13438 Class A • ICES-003 Class A
System architecture	Nonblocking shared-memory switch
System processor	IBM Power PC 405GP, 200 MHz CPU
ANSI Fibre Channel protocol	FC-PH (Fibre Channel Physical and Signaling Interface standard)
Modes of operation	Fibre Channel Class 2, Class 3, and Class F
Fabric initialization	Complies with FC-SW 5.0
Internet protocol (IP) over Fibre Channel (FC-IP)	Complies with FC-IP 2.3 of the FCA profile
Aggregate switch input/output (I/O) bandwidth	Per port: 4 Gbps, running at 2 Gbps, full duplex Per 16-port card: 64 Gbps, all 16 ports at 2 Gbps, full duplex
Port-to-port latency	Less than 2 microseconds with no contention (destination port is free)
Data transmission range	• Up to 500 m (1625 ft) for short wavelength optical link • Up to 10 km (32 820 ft) for long wavelength optical link
Immunity	• IEC 61000-4-2 Severity Level 3 for Electrostatic Discharge • IEC 61000-4-3 Severity Level 3 for Radiated Fields • IEC 61000-4-4 Severity Level 3 for Fast Transients • IEC 61000-4-5 Severity Level 3 for Surge Voltage • IEC 61000-4-6 Conducted Emissions • IEC 61000-4-11 Voltage Variations

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 1190 Doc: 3698

Table 21. General specifications (continued)

Specification	Description
Acoustics	When measured in EIA 4 of a 36 EIA TotalStorage rack, with front cover, and rear cover with acoustic baffle, declared sound power is LwAd = 7.5 B, average bystander sound pressure is LpA = 59 dBA.
Routing capacity	A minimum aggregate routing capacity of four million frames per second is provided for Class 2, Class 3, and Class F frames in a 64-port switch.

Regulatory specifications

The 2109 Model M12 is certified for the regulatory specifications that are listed in Table 22.

Table 22. Regulatory specifications

Country or region	Safety specification	EMC specification
Canada	CSA 22.2 No. 60950 Third Ed.	ICES-003 Class A
United States	UL 60950 Third Ed., Info. Tech. Equip.	FCC Part 15, Subpart B, (CFR title 47) Class A
Japan	IEC 60950+A1+A2+A3+A4+A11	VCCI V-3/2000.04, Class A
International	IEC 60950+A1+A2+A3+A4+A11	CISPR22 Class A
Norway	Nemko IEC 60950+A1+A2+A3+A4+A11 (CB Report)	

Table 22. Regulatory specifications (continued)

Country or region	Safety specification	EMC specification
European Union (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom)	73/23/EEC based on compliance to EN 60950:92 +A1:93+A2:93+A3:95+ A4:96+A11:97 (CB report inclusive of county deviations); TUV-GS (Germany)	89/336/EEC EN 55022:1998 Class A EN 55024 (Immunity) EN 60825-1:1994/A11, -2 EN 61000-4-2 Severity Level 3 for Electro Static Discharge EN 61000-4-3 Severity Level 3 for Radiated Fields EN 61000-4-4 Severity Level 3 for Electrical Fast Transients EN 61000-4-5 Severity Level 3 for Surge Voltage EN 61000-4-6 Conducted Emissions EN 61000-4-8 Magnetic Fields EN 61000-4-11 Line Interruption
Taiwan		BSMI Certification CNS 13438
Australia and New Zealand		AS/NZS 3548:1995 Class A (radio interference)

The 2109 Model C36 is certified for the following regulatory specifications:

- IEC 60950/EN 60950 Third Ed.
- CSA 60950-00/ANSI-UL 60950 Third Ed.
- CE (7/23/EEC based on EN 60950 Third Ed.; 89/336/EEC)

POST and Boot specifications

The Model M12 performs a POST by default each time that you power on (cold boot) or restart or reset the chassis. You can restart the Model M12 with the **switchreboot** command, the **reboot** command, or the **fastboot** command. The **fastboot** command restarts the switches without running POST. If you restart the active CP card, it fails over to the standby CP card.

Monitoring POST results

You can monitor the success and failure of the diagnostic tests that are run during POST through LED activity, the error log, or a command line interface. POST requires a minimum of 3 minutes to complete, however the time might vary depending on the devices that are connected to the 2109 Model M12.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1191
Doc: 3698

POST performs the following steps:

1. Runs preliminary POST diagnostics
2. Initializes the operating system
3. Initializes the hardware
4. Runs diagnostic tests on several functions, including circuitry, port functionality, ability to send and receive frames, all aspects of memory, parity, statistics counters, and serialization

Boot

Boot completes in a minimum of 3 minutes if you run a POST. In addition to POST, boot includes the following steps after the POST completes:

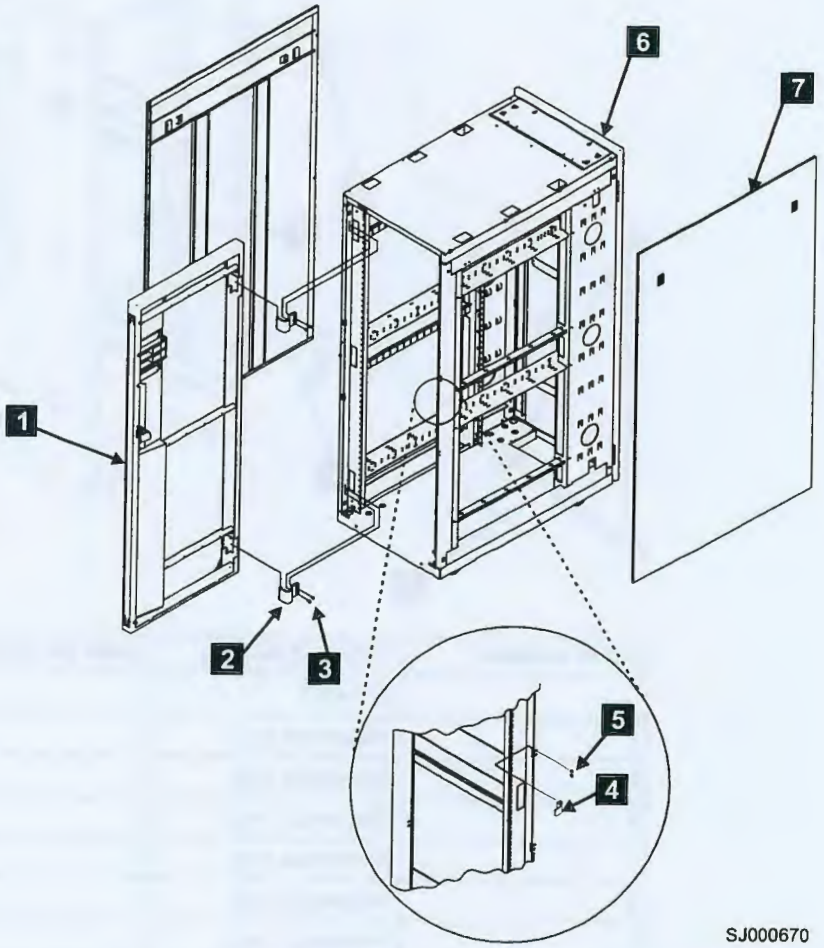
1. Configures the universal port
2. Initializes the links
3. Analyzes the fabric. If any ports are connected to other switches, the switch participates in a fabric configuration.
4. Obtains a domain ID for the switch and assigns port addresses
5. Constructs unicast routing tables
6. Enables normal port operation

10898 Paula

Appendix B. Parts information

This appendix contains detailed drawings, field replaceable unit (FRU) part numbers, and part descriptions for a 2109 Model C36 with Model M12.

Covers



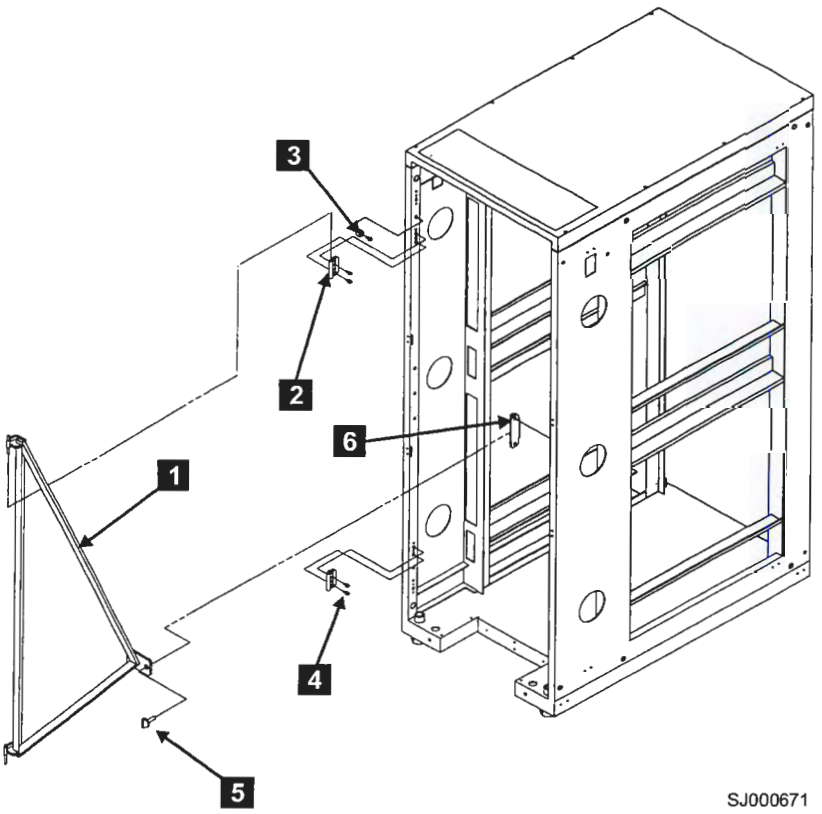
SJ000670

Index number	FRU part number	Units per assembly	Description
1	18P2120	1	Front door
2	31L7547	2	Hinge, front door
3	31L8594	4	Screw, front hinge
4	31L7545	1	Latch, front door
5	31L7540	2	Screw, front door latch
6	11P0724	1	Rear door (black)
7	05N6478	2	Side panel (black)

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1192
Doc. 3698

Earthquake brace

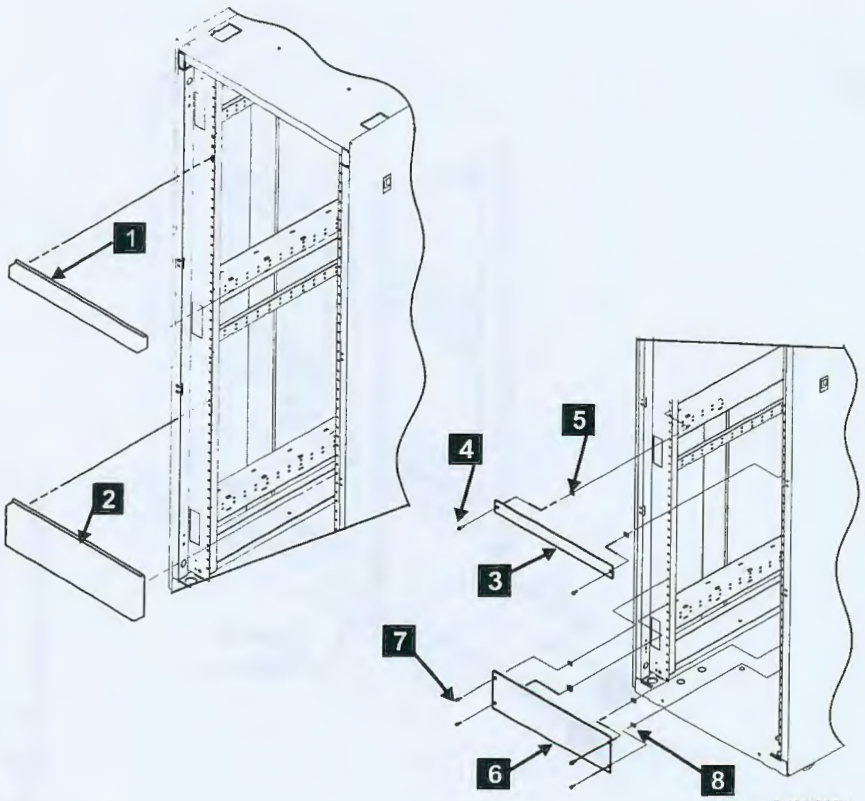


SJ000671

Index number	FRU part number	Units per assembly	Description
	05N4697	1	Earthquake brace kit
1	Reference only	1	Bracket
2	Reference only	2	Hinge
3	Reference only	1	Spacer
4	Reference only	7	Screw
5	Reference only	1	Bolt
6	Reference only	1	Latch plate

10896 Paula

Blank fillers

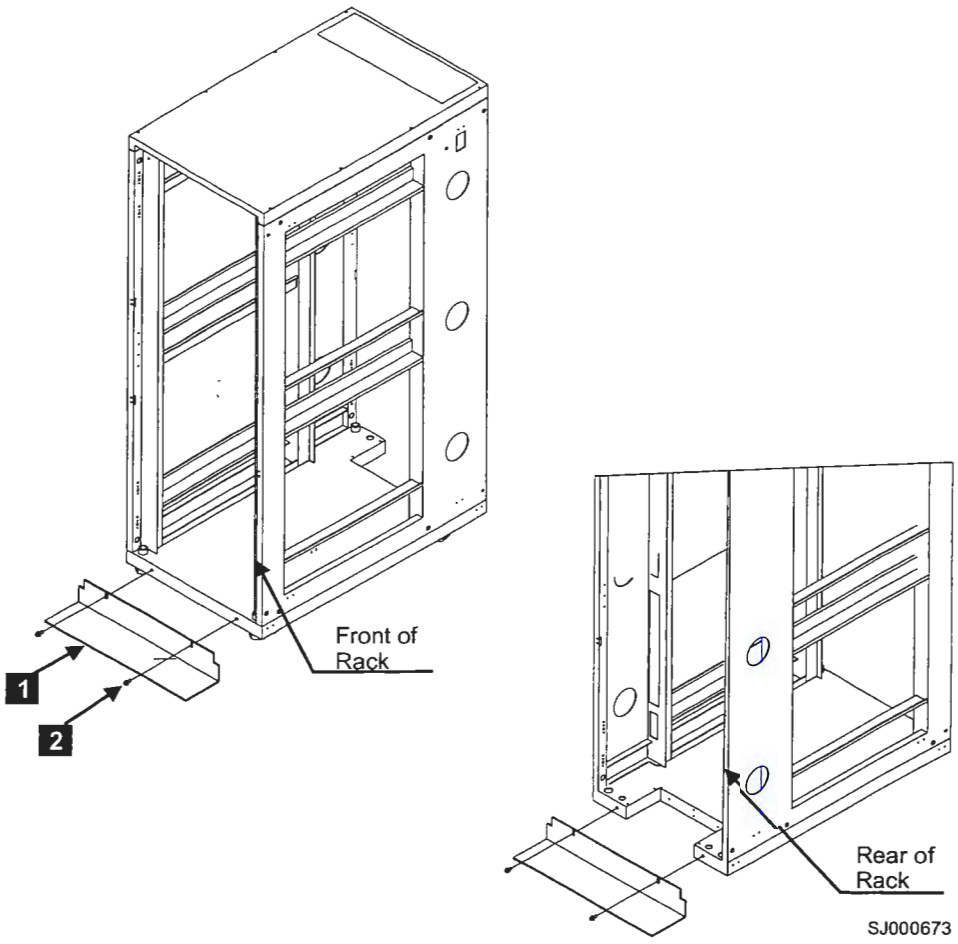


SJ000672

Index number	FRU part number	Units per assembly	Description
1	97H9754	As needed	1U (black) filler snap
2	97H9755	As needed	3U (black) filler snap
	18P2265	As needed	1U bolt in panel kit, (black)
3	Reference only	1	Panel (1U kit)
4	Reference only	2	M5 X 14 Hex screw (1U kit)
5	Reference only	2	M5 nut clip (1U kit)
	18P2233	As needed	3U bolt in panel kit, (black)
6	Reference only	1	Panel (3U kit)
7	Reference only	4	M5 X 14 hex screw (3U kit)
8	Reference only	4	M5 nut clip (3U kit)

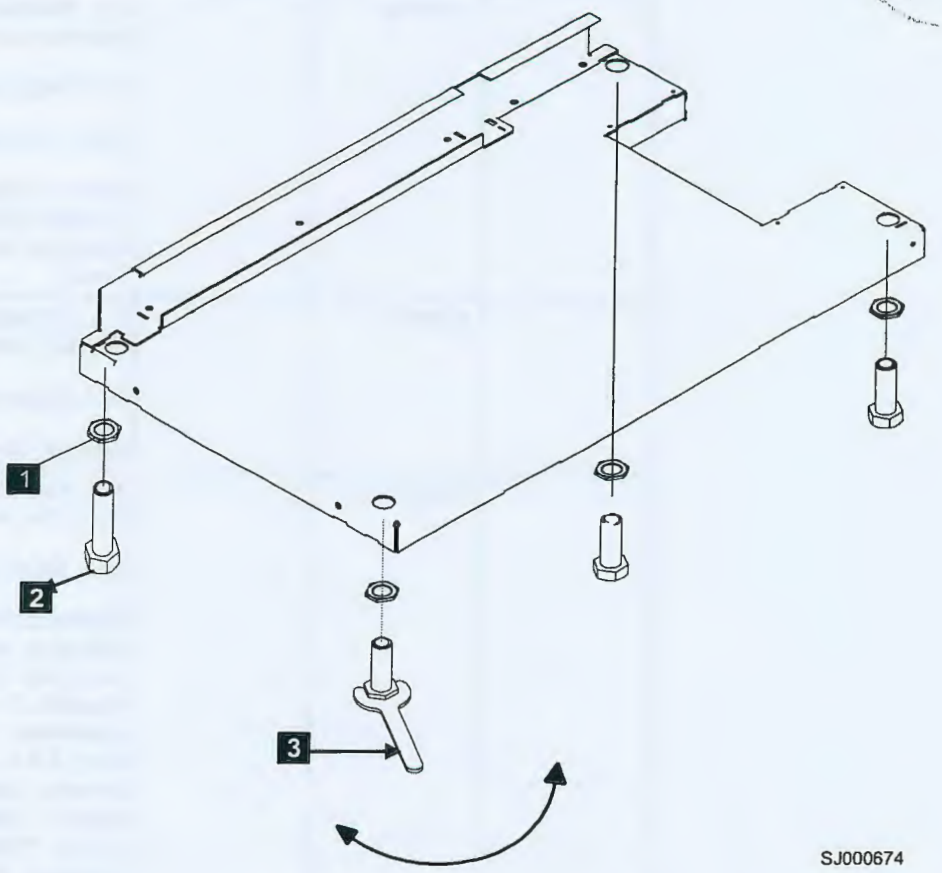
RQS nº 03/2005 CN
Fls. Nº 1193
Doc. 3698

Stabilizers



Index number	FRU part number	Units per assembly	Description
	31L8305	1	Stabilizer kit (black)
1	Reference only	2	Bracket
2	Reference only	4	M8 X 25 screw, button head socket

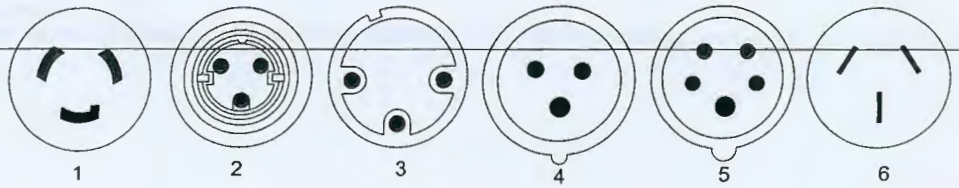
Leveling feet



SJ000674

Index number	FRU part number	Units per assembly	Description
1	Reference only	4	Jam nut
2	Reference only	4	Leveller
3	31L8313	1	Wrench

Power cords



SJ000675

Index number	FRU part number	Units per assembly	Country or region
1	11F0113	1	U.S. Standard, type 12 plug, L6-30P twist-lock connector, 14 ft cord 30 A, single phase U.S.A., Canada Anguilla, Antigua, Cape Verde Islands, Cayman Islands, French Polynesia, Honduras, Montserrat, St. Kitts and Nevis, Tortola
1	11F0114	1	U.S., Chicago, type 12 plug, L6-30P twist-lock connector, 6 ft cord 30 A, single phase Chicago, Illinois, U.S.A.
1	11F0115	1	AFE, type 12 plug, L6-30P twist-lock connector, 14 ft cord 30 A, single phase Argentina, Bahamas, Bangladesh, Barbados, Bermuda, Bolivia, Chile, China, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Honduras, Hong Kong S.A.R. of China, India, Indonesia, Jamaica, Japan, Macau S.A.R. of China, Malaysia, Mexico, Myanmar, Netherlands Antilles, Panama, Peru, Philippines, Singapore, Sri Lanka, Suriname, Taiwan, Thailand, Trinidad, Venezuela
N/A	18P2257	1	Universal without wall plug connector (non-US or Canada)
3	11F0106	1	30 A, single phase, PDL connector Wilco WP, type PDL plug, 14 ft cord Australia
3	11F0107	1	30 A, single phase, PDL connector Wilco WP, type PDL plug, right angle, 14 ft cord New Zealand

10892 Paula

Index number	FRU part number	Units per assembly	Country or region
4	31F4466	1	32 A, single phase, three pin connector IEC 309, type 46 connector (2 power + ground), 14 ft cord Belgium, Bahrain, Botswana, Brazil, Egypt, Ethiopia, France, Ghana, Germany, Greece, Iceland, Iraq, Ireland, Italy, Jordan, Kenya, Kuwait, Lebanon, Malawi, Nigeria, Norway, Oman, Qatar, Saudi Arabia, Spain, Sudan, Tanzania, Uganda, United Kingdom, United Arab Emirates, Zaire, Zambia, Zimbabwe
N/A (See Note)	18P2257	1	Switzerland
6	87G6067	1	30 A, single phase Type KP connector, right angle, 14 ft cord Korea
Note: Install according to the national electrical code of the specific country or region.			

Cabinet parts list

Table 23 lists the items that are supplied with the 14U chassis mount kit.

Table 23. Items supplied with the 14U chassis mount kit

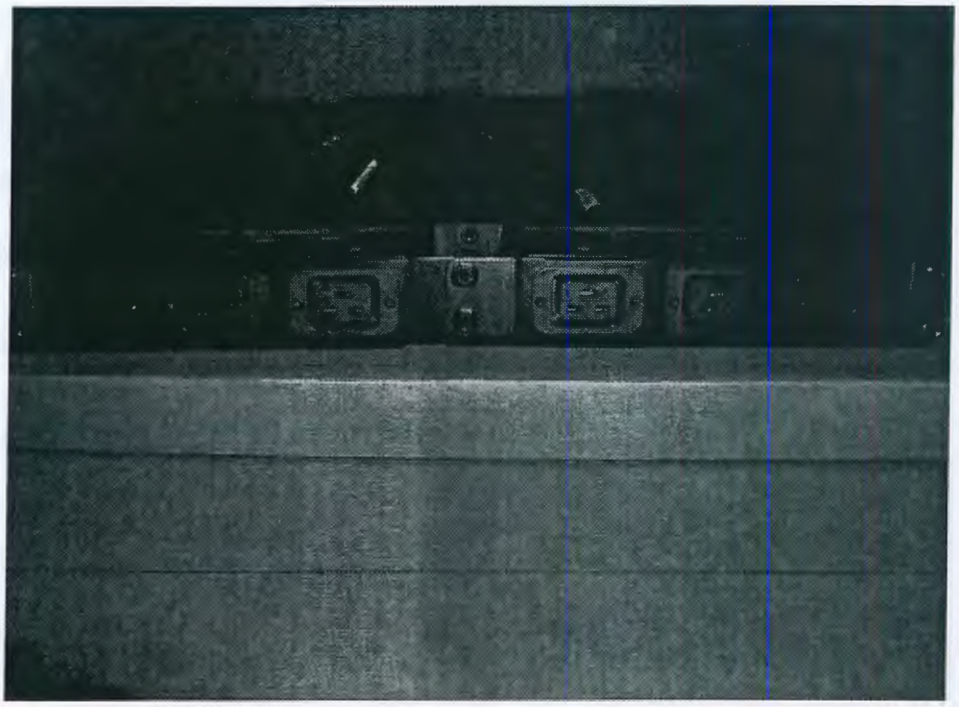
Item No.	Description	Quantity
1	Left mount shelf bracket	1
2	Right mount shelf bracket	1
3	Left upper mount bracket assembly, containing:	1
3a	Left upper mount bracket (flat)	1
3b	Left upper mount bracket (L-shaped)	1
3c	Screw	2
4	Right upper mount bracket assembly, containing:	1
4a	Right upper mount bracket (flat)	1
4b	Right upper mount bracket (L-shaped)	1
4c	Screw	2
5	10-32 x 5/16-in. Phillips flathead screw	8
6	10-32 x 5/8 in. Phillips panhead screw with washer	4
7	10-32 clip nut (package of 20; only four are required)	20

RQS nº 03/2005 - CN
Fls. Nº 1195
Doc 3698

Table 23. Items supplied with the 14U chassis mount kit (continued)

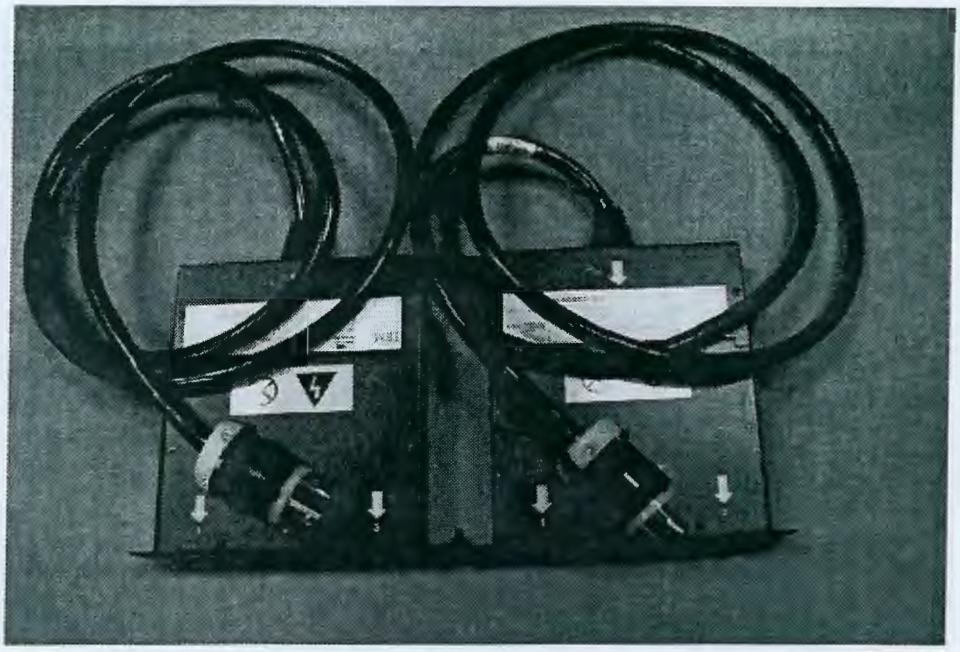
Item No.	Description	Quantity
8	1/4-20 x 1/2 in. Phillips panhead screws, with lock washer	16
Discard the following		
9	10-32 retainer nuts	4
10	1/4-20 x 1/2 in. Phillips panhead screws with glue	16
11	0.375 in. square washers	16
12	8-32 x 5/16 in. Phillips flathead screws	8

Power distribution unit (PDU)



SJ000652

Figure 57. Front view of the PDU



SJ000653

Figure 58. Top view of the PDU

FRU part number	Units per assembly	Description
32P1077	2 each	PDU, Winchester (PDU chassis)
24P6847	2 each	Power cord, PDU

2109 Model M12 parts list

FRU part number	Units per assembly	Description
18P5017	4 each	Switch blade, 16 port, 2 GB
18P5032	1 each	Chassis door
18P5034	4 each	Filler panel, switch blade, 16 port, 2 GB
18P5035	2 each	Blade, control processor
18P5037	3 each	Power supply, 180 - 264 V ac, 1000 watts
18P5039	3 each	Blower assembly
18P5126	1 each	Rear LED status panel card
18P5128	1 each	Chassis (including the backplane, blower and power supply backplane, ac and blower harness)
18P5130	1 each	Rear WWN bezel
18P5131	1 each	Tray, cable management

RQS nº 03/2005 - CN
(PMI - CORREIOS
Fls Nº 1196
Doc 3698

Appendix C. Blank planning worksheets

This appendix contains the following blank worksheets that you can use when you plan the installation of a 2109 Model C36 with Model M12:

- Planning worksheet
- Port configuration worksheet
- Zone definition worksheet
- Zone configuration worksheet

Make as many copies of the blank worksheets as you need to plan the installation of your switches. Give your system administrator copies of the completed worksheets.

Planning worksheet

Table 24. Planning worksheet

Item	Description
Firmware level	
Firmware location:	
Server name	
Username	
Directory	
Switch name	
Domain ID	
FCnetID (Fibre Channel IP address)	
FC netmask	
WWN	
Role	
Syslog daemon IP address	
Users defined - access level	
SNMP information:	
System description	
System contacts	
System location	
Event trap level 0 - 5	
Enable authentication traps	
RW community string	
RO community string	
Trap recipients IP address	
License keys	

© Copyright IBM Corp. 2002, 2003

10887 Paula

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1197
Doc. 3698

Port configuration worksheet

Table 25. Port configuration worksheet

Port number	Device name	Device port	Cable length	Port type	Notes	Cable number
0						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Zone definition worksheet

Table 26. Zone definition worksheet

Zone member type (switch, port, WWN)	Zone member	Zone configuration name	Comments
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1198
Doc. 3698

Zone configuration worksheet

Table 27. Zone configuration worksheet

Zone member type (switch, port, WWN)	Zone member	Zone configuration name	Connects to
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			

10.885 Paula

Notices

This information was developed for products and services offered in the U. S. A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1199 123
Doc: 3698

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM
TotalStorage

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission statements

This section gives the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada compliance statement

Avis de conformite a la reglementation d'Industrie Canada: Cet appareil numerique de la classe A est conform a la norme NMB-003 du Canada.

Chinese Class A compliance statement

Attention: This is a Class A statement. In a domestic environment, this product might cause radio interference in which case the user might be required to take adequate measures.

ANATEL
10.883
2

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

European Community compliance statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product is in conformity with the EU council directive 73/23/EEC on the approximation of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits. This conformity is based on compliance with the following harmonized standard: EN60950.

This product has been tested and found to comply with the limits for class A Information Technology Equipment according to European Standard EN 55022. The limits for class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Where shielded or special cables (for example, cables fitted with ferrites) are used in the test to make the product comply with the limits:

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

Germany compliance statement

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische

Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

~~Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG~~ das

EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuellt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Notices
Fls Nº 1200
Doc. 3698

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:_|t¹|

"Geraete duerfen an Orten, fuer die sie nicht ausreichend entstoert sind, nur mit besonderer Genehmigung des Bundesministeriums fuer Post und Telekommunikation oder des Bundesamtes fuer Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Stoerungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs.4)

Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden

Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Nach der EN 55022:

"Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstoerungen verursachen. in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzufuehren und dafuer aufzukommen."

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen, sind die Geraete wie in den Handbuechern angegeben zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Government Ministry of Communication (MOC) statement

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this is not suitable for your use, you may exchange it for one with a non-business use.

Taiwan class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。 VS07171L

Glossary

This glossary provides definitions for the Fibre Channel and switch terminology used for the IBM 2109 Model M12. This glossary also provides definitions for the Fibre Channel and switch terminology used for the IBM TotalStorage SAN Cabinet 2109 Model C36.

This glossary defines technical terms and abbreviations used in this document. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at www.ibm.com/networking/nsg/nsgmain.htm

This glossary also includes terms and definitions from:

- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms.* New York: McGraw-Hill, 1994.

The following cross-reference conventions are used in this glossary:

See Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

See also Refers you to a related term.

8b/10b encoding. An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports

16-port card. The Fibre Channel port card provided with the 2109 Model M12. Contains 16 ports and the corresponding light-emitting diodes (LEDs). See also *port card.*

access control list (ACL). Enables an organization to bind a specific worldwide name (WWN) to a specific switch port or set of ports, preventing a port in another physical location from assuming the identity of a real WWN. Can also refer to a list of the read/write access of a particular community string. See also *device connection controls.*

account level switches. Switches that have four login accounts into the operating system (in descending order): root, factory, admin, and user. See also *admin account.*

ACL. See *access control list.*

address identifier. A 24-bit or 8-bit value used to identify the source or destination of a frame.

admin account. A login account intended for use by the customer to control switch operation. See also *account level switches.*

alias. An alternate name for an element or group of elements in the fabric. Aliases can be used to simplify the entry of port numbers and worldwide names (WWNs) when creating zones.

alias address identifier. An address identifier recognized by a port in addition to its standard identifier. An alias address identifier can be shared by multiple ports.

alias AL_PA. An arbitrated loop physical address (AL_PA) value recognized by a loop port (L_port) in addition to the AL_PA assigned to the port. See also *arbitrated loop physical address.*

alias server. A fabric software facility that supports multicast group management.

AL_PA. See *arbitrated loop physical address.*

American National Standards Institute (ANSI). The governing body for Fibre Channel standards in the U.S.A.

ANSI. See *American National Standards Institute.*

API. See *application programming interface.*

application programming interface (API). A defined protocol that allows applications to interface with a set of services.

application-specific integrated circuit (ASCI). In computer chip design, an integrated circuit created by first mounting an array of unconnected logic gates on a substrate and later connecting these gates in a particular configuration for a specific application. This design approach allows chips for a variety of applications to be made from the same generic gate array, thereby reducing production costs

ARB. See *arbitrate primitive signal.*

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1201
Doc. 3698

arbitrate primitive signal (ARB). A primitive signal that is transmitted as the fill word by a loop port (L_port) to indicate that the L_port is arbitrating to access to the loop. Applies only to the arbitrated loop topology.

arbitrated loop. A shared 100 MBps Fibre Channel transport structured as a loop and supporting up to 126 devices and one fabric attachment. A port must successfully arbitrate before a circuit can be established.

arbitrated loop physical address (AL_PA). An 8-bit value used to uniquely identify an individual port within a loop. A loop can have one or multiple AL_PAs.

arbitration wait timeout value (AW_TOV). The minimum time an arbitrating loop port (L_port) waits for a response before beginning loop initialization.

area number. A number that is assigned to each potential port location in the switch. Used to distinguish ports that have the same port number but are on different port cards.

ASIC. See *application-specific integrated circuit.*

asynchronous transfer mode (ATM). A broadband technology for transmitting data over local area networks (LANs) or wide area networks (WANs), based on relaying cells of fixed size. Provides any-to-any connectivity, and nodes can transmit simultaneously.

ATM. See *asynchronous transfer mode.*

auto-negotiate speed. Process that allows two devices at either end of a link segment to negotiate common features, speed (for example, 1 Gbps or 2 Gbps) and functions.

autoranging. A power supply that accommodates different input voltages and line frequencies.

autosense. Process during which a network device automatically senses the speed of another device.

AW_TOV. See *arbitration wait timeout value.*

backup FCS switch. The switch or switches assigned as backup in case the primary fabric configuration server (FCS) switch fails. See also *fabric configuration server switch* and *primary FCS switch.*

bandwidth. (1) The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). (2) The range of transmission frequencies available to a network. See also *throughput.*

basic input/output system (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BB_credit. See *buffer-to-buffer credit.*

beacon. When all the port light-emitting diodes (LEDs) on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by Telnet command or through Web Tools.

beginning running disparity. The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. See also *disparity.*

BER. See *bit error rate.*

BIOS. See *basic input/output system.*

BISR. Built-in self-repair.

bit error rate (BER). The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted. See also *error.*

blade. One component in a system that is designed to accept some number of components (blades). Blades could be individual servers that plug into a multiprocessing system or individual port cards that add connectivity to a switch. A blade is typically a hot swappable hardware device. See *16-port card.*

blind-mate connector. A two-way connector used in some switches to provide a connection between the system board and the power supply.

block. As applies to fibre channel, upper-level application data that is transferred in a single sequence.

bloom. Application-specific integrated circuit (ASIC) technology that the 2109 Model M12 is based on.

boot flash. Flash memory that stores the boot code and boot parameters. The processor runs its first instructions from boot flash. Data is cached in random access memory (RAM).

boot monitor. Code used to initialize the control processor (CP) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

British thermal unit (BTU). A measurement of heat produced in one hour.

broadcast. The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *multicast* and *unicast.*

BTU. See *British thermal unit.*

buffer-to-buffer credit. The number of frames that can be transmitted to a directly-connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. See also *buffer-to-buffer flow control.*

10879

buffer-to-buffer flow control. Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. See also *buffer-to-buffer credit.*

CAM. Content addressable memory.

cascade. Two or more interconnected Fibre Channel switches that can build large fabrics. Switches can be cascaded up to 239 switches, with a recommended maximum of seven inter-switch links (no path longer than eight switches). See also *fabric* and *inter-switch link.*

central processing unit (CPU). A part of a computer that includes the circuits that control the interpretation and execution of instructions. A CPU in the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

chassis. The metal frame in which the switch and switch components are mounted.

circuit. An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions. See also *link.*

class 1. Service that provides a dedicated connection between two ports (also called connection-oriented service), with notification of delivery or nondelivery.

class 2. Connectionless service between ports with notification of delivery or nondelivery.

class 3. Connectionless service between ports without notification of delivery. Other than notification, the transmission and routing of class 3 frames is the same as class 2 frames.

class F. Connectionless service for inter-switch control traffic. Provides notification of delivery or nondelivery between two expansion ports (E_ports).

class of service. A specified set of delivery characteristics and attributes for frame delivery.

CLI. See *command line interface.*

CMI. Control message interface.

comma. A unique pattern (either 1100000 or 0011111) used in 8b/10b encoding to specify character alignment within a data stream. See also *K28.5.*

command line interface (CLI). Interface that depends entirely on the use of commands, such as through Telnet or simple network management protocol (SNMP), and does not involve a graphical user interface.

community (SNMP). A relationship between a simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

compact flash. Flash memory that stores the run-time operating system and is used like hard disk storage. Not visible within the memory space of the processor. Data is stored in file system format. Also called user flash.

control processor (CP). The central processing unit that provides all control and management functions in a switch.

control processor card (CP card). The central processing unit of the 2109 Model M12, which contains two control processor (CP) card slots to provide redundancy. Provides Ethernet, serial, and modem ports with the corresponding light-emitting diodes (LEDs).

core switch. A switch whose main task is to interconnect other switches. Also referred to as a backbone switch. See also *edge switch.*

CP. See *control processor.*

CP card. See *control processor card.*

CPLD. Complex programmable logic device.

CPU. See *central processing unit.*

CRC. See *cyclic redundancy check.*

credit. When applied to a switch, the maximum number of receive buffers provided by a fabric port (F_port) or fabric loop port (FL_port) to its attached node port (N_port) or node loop port (NL_port), respectively, such that the N_port or NL_port can transmit frames without over-running the F_port or FL_port.

CSA. Canadian Standards Association.

cut-through. A switching technique that allows the route for a frame to be selected as soon as the destination address is received. See also *route.*

cyclic redundancy check (CRC). A check for transmission errors included in every data frame.

data communications equipment (DCE) port. A port that is capable of interfacing between a data terminal equipment (DTE) port and a transmission circuit. DCE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *data terminal equipment (DTE) port.*

data rate. The rate at which data is transmitted or received from a device. Interactive applications tend to require a high data rate, while batch applications can usually tolerate lower data rates.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1202
Doc. 3698

data terminal equipment (DTE) port. A port that is capable of interfacing to a transmission circuit through a connection to a data communications equipment (DCE) port. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2 in a 9-pin connector (reversed in 25-pin connectors). See also *data communications equipment (DCE) port.*

DB-9 connector. A 9-pin version of the RS-232C port interface.

DCC. A dc converter.

DCE port. See *data communications equipment (DCE) port.*

DDR. Double data rate. See *data rate.*

defined zone configuration. The complete set of all zone objects that are defined in the fabric. The defined configuration can include multiple zone configurations. See also *enabled zone configuration* and *zone configuration.*

device. Hosts and storage that connect to a switch. Example devices are servers, redundant array of independent disks (RAID) arrays, and tape subsystems.

device connection controls. Enables organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by a worldwide name (WWN) and typically represent host bus adapters (HBAs) (servers). See also *access control lists.*

DID. The 3-byte destination ID of the destination device, in the 0xDomainAreaALPA format.

direct memory access (DMA). The transfer of data between memory and an input/output device without processor intervention.

disparity. The relationship of ones and zeros in an encoded character. *Neutral disparity* means an equal number of each, *positive disparity* means a majority of ones, and *negative disparity* means a majority of zeros.

DLS. See *dynamic load sharing.*

DMA. See *direct memory access.*

DNS. Distributed name server.

domain_ID. Unique identifier for the switch in a fabric. Usually automatically assigned by the switch, but can also be assigned manually. Can be any value between 1- 239.

DRAM. See *dynamic random access memory.*

DTE port. See *data terminal equipment (DTE) port.*

dual fabric. Two identical fabrics that allow redundancy in the event that one fabric fails. Use a dual fabric for mission critical applications.

dual-fabric SAN. A storage area network (SAN) that is composed of two independent fabrics. Synonymous with multi-fabric SAN. The two-fabric architecture makes dual-fabric SANs redundant.

DWDM. Dense wavelength digital multiplexing.

dynamic load sharing (DLS). Dynamic distribution of traffic over available paths. Allows for recomputing of routes when a fabric port or fabric loop port (Fx_port) or expansion port (E_port) changes status.

dynamic random access memory (DRAM). A storage in which the cells require repetitive application of control signals to retain stored data.

edge fabric. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric. See also *resilient core.*

edge switch. A switch whose main task is to connect nodes into the fabric. See also *core switch.*

E_D_TOV. See *error detect timeout value.*

EE_credit. See *end-to-end credit.*

effective zone configuration. The particular zone configuration that is currently in effect. Only one configuration can be in effect at once. The effective configuration is built each time a zone configuration is enabled.

EIA. Electronic Industry Association.

EIA rack. A storage rack that meets the standards set by the Electronics Industry Association (EIA).

electromagnetic compatibility (EMC). The design and test of products to meet legal and corporate specifications dealing with the emissions and susceptibility to frequencies in the radio spectrum. Electromagnetic compatibility is the ability of various electronic equipment to operate properly in the intended electromagnetic environment.

electromagnetic interference (EMI). Waves of electromagnetic radiation, including but not limited to radio frequencies, generated by the flow of electric current.

electrostatic discharge (ESD). The flow of current that results when objects having a static charge come into close enough proximity to discharge.

ELP. Extended link parameters.

ELWL. See *extra long wavelength.*

EMC. See *electromagnetic compatibility.*

EMI. See *electromagnetic interference.*

enabled zone configuration. The currently enabled configuration of zones. Only one configuration can be enabled at a time. See also *defined zone configuration* and *zone configuration.*

end port. A port on an edge switch that connects a device to the fabric.

end-to-end credit (EE_credit). The number of receive buffers allocated by a recipient port to an originating port. Used by class 1 and class 2 services to manage the exchange of frames across the fabric between source and destination. See also *end-to-end flow control* and *buffer-to-buffer credit.*

end-to-end flow control. Governs flow of class 1 and class 2 frames between node ports (N_ports). See also *end-to-end credit.*

E_port. See *expansion port.*

error. As applies to fibre channel, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors). See also *loop failure.*

error detect timeout value (E_D_TOV). The time that the switch waits for an expected response before declaring an error condition. Adjustable in 1 microsecond increments from 2 - 10 seconds.

ESD. See *electrostatic discharge.*

exchange. The highest level Fibre Channel mechanism used for communication between node ports (N_ports). Composed of one or more related sequences, and can work in either one or both directions.

expansion port (E_port). A port is designated an expansion port (E_port) when it is used as an inter-switch expansion port to connect to the E_port of another switch, to build a larger switch fabric.

Extended Fabrics. A feature that runs on Fabric operating system (OS) and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 km (62.14 mi).

extra long wavelength (ELWL). Laser light with a periodic length greater than 1300 nm (for example, 1420 or 1550). ELWL lasers are used to transmit Fibre Channel data over distances greater than 10 km. Also known as XLWL.

fabric. A network that uses high-speed fibre connections to connect switches, hosts, and devices. A fabric is an active, intelligent, nonshared interconnect scheme for nodes.

Fabric Access. Allows the application to control the fabric directly for functions such as discovery, access (zoning) management, performance, and switch control. Consists of a host-based library that interfaces the application to switches in the fabric over an out-of-band TCP/IP connection or in-band using an IP-capable host bus adapter (HBA).

Fabric Assist. A feature that enables private and public hosts to access public targets anywhere on the fabric, provided they are in the same Fabric Assist zone.

fabric configuration server (FCS) switch. One or more designated switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by worldwide name (WWN), and the list of designated switches is communicated fabric-wide. See also *backup FCS switch*, *primary FCS switch.*

fabric login (FLOGI). The process by which a device gains access to the fabric.

fabric loop port (FL_port). A fabric port that is loop capable. Used to connect node loop ports (NL_ports) to the switch in a loop configuration.

Fabric Manager. A feature that allows the storage area network (SAN) manager to monitor key fabric and switch elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values or counters and provides notification when defined boundaries are exceeded. The SAN manager can configure which elements, such as error, status, and performance counters, are monitored within a switch.

fabric mode. One of the modes for a loop port (L_port). An L_port is in fabric mode when it is connected to a port that is not loop capable and is using fabric protocol. See also *loop port* and *loop mode.*

fabric name. The unique identifier assigned to a fabric and communicated during login and port discovery.

Fabric OS. An operating system made up of two software components: the firmware that initializes and manages the switch hardware, and diagnostics.

fabric port (F_port). A port that is able to transmit under fabric protocol and interface over links. Can be used to connect a node port (N_port) to a switch. See also *fabric loop port* and *Fx_port.*

Fabric Watch. A feature that runs on Fabric operating system (OS) and allows monitoring and configuration of fabric and switch elements.

failover. The act that causes control to pass from one redundant unit to another.

FAN. Fabric address notification.

FC. See *fibre channel.*

FCA. See *Fibre Channel arbitrated loop.*

FC-AL. See *Fibre Channel arbitrated loop.*

ECT 10.877 J

BOS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1203
Doc. 3698

FC-AL-3. The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCC. Federal Communications Commission.

FC-FLA. The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCMGMT. Fibre Alliance Fibre Channel Management.

FCP. See *Fibre Channel protocol.*

FC-PDLA. The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FC-PH-1,2,3. The Fibre Channel Physical and Signaling Interface standards defined by ANSI.

FC-PI. The Fibre Channel Physical Interface standard defined by ANSI.

FCS switch. See *fabric configuration server switch.*

FC-SW-2. The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches in order to create a multiswitch Fibre Channel fabric.

fibre channel (FC). A technology for transmitting data between computer devices at a data rate of up to 4 Gbps. It is especially suited for attaching computer servers to shared storage devices and for interconnecting storage controllers and drives.

Fibre Channel arbitrated loop (FC-AL). A standard defined on top of the FC-PH standard. It defines the arbitration on a loop where several FC nodes share a common medium.

Fibre Channel protocol (FCP). The protocol for transmitting commands, data, and status using Fibre Channel FC-FS exchanges and information units. Fibre channel is a high-speed serial architecture that allows either optical or electrical connections at data rates from 265 Mbps up to 4-Gbps.

Fibre Channel service (FS). A service that is defined by Fibre Channel standards and exists at a well-known address. For example, the Simple Name Server is a Fibre Channel service. See also *Fibre Channel service protocol.*

Fibre Channel service protocol (FSP). The common protocol for all fabric services, transparent to the fabric type or topology. See also *Fibre Channel service.*

Fibre Channel shortest path first (FSPF). A routing protocol used by Fibre Channel switches.

Fibre Channel transport. A protocol service that supports communication between Fibre Channel service providers. See also *Fibre Channel service protocol.*

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit can contain other field replaceable units.

File Transfer protocol (FTP). In Transmission Control protocol/Internet protocol (TCP/IP), an application protocol used for transferring files to and from host computers.

fill word. An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

firmware. The basic operating system provided with the hardware.

FLA. Fabric loop attach.

flash partition. Two redundant usable areas, called *partitions* into which firmware can be downloaded in the 2109 Model M12.

FLOGI. See *fabric login.*

FL_port. See *fabric loop port.*

F_port. See *fabric port.*

frame. The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, the data payload, a cyclic redundancy check (CRC), and an end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements, and so on) and data frames.

frame delimiter. A part of an ordered set that marks frame boundaries and describes frame contents. See also *ordered set.*

FRU. See *field replaceable unit.*

FS. See *Fibre Channel service.*

FSP. See *Fibre Channel service protocol.*

FSPF. See *Fibre Channel shortest path first.*

FTP. See *File Transfer protocol.*

full duplex. A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *half duplex.*

Fx_port. A fabric port that can operate as either a fabric port (F_port) or fabric loop port (FL_port). See also *fabric port* and *fabric loop port.*

gateway. Hardware that connects incompatible networks by providing the necessary translation for both hardware and software.

GBIC. See *gigabit interface converter.*

Gbps. Gigabits per second.

GBps. Gigabytes per second.

generic port (G_port). A generic port that can operate as either an expansion port (E_port) or a fabric port (F_port). A port is defined as a G_port when it is not yet connected or has not yet assumed a specific function in the fabric.

gigabit interface converter (GBIC). A removable serial transceiver module designed to provide gigabaud capability for fibre channel (FC) and other products that use the same physical layer.

gigabit switch. A 16-port, Fibre Channel gigabit switch.

G_port. See *generic port.*

half duplex. A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time). See also *full duplex.*

hard address. The arbitrated loop physical address (AL_PA) that a node loop port (NL_port) attempts to acquire during loop initialization.

hardware translative mode. Method for achieving address translation. The two hardware translative modes that are available to a QuickLoop-enabled switch are standard translative mode and QuickLoop mode. See also *standard translative mode* and *QuickLoop mode.*

HBA. See *host bus adapter.*

heartbeat. Through clustering software, the application server continually communicates with the clustered spare using network heartbeats to indicate to the other machines that everything is operating correctly. This heartbeat is typically carried over a dedicated network for clustering traffic. In cases of a problem (for example, a software crash on the operational server or a hardware component failure), a heartbeat link indicates to the other server that something has failed or is otherwise inoperative. If that heartbeat is lost, the spare server takes over the function provided by the application service. Depending on the clustering software, either the entire server or only specific services on the server can be failed over or failed back.

high availability. An attribute of the switch that identifies it as being capable of operating well in excess of 99 percent of the time. High Availability is typically identified by the number of nines in that percentage. For example, a switch that is rated at five nines would be capable of operating 99.999 percent of the time without failure.

high port count fabric. A fabric containing 100 or more ports.

host bus adapter (HBA). The interface card between a server or workstation bus and the Fibre Channel network.

hot pluggable. A field replaceable unit (FRU) capability that indicates it can be extracted or installed while customer data is otherwise flowing in the chassis.

hub. A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

IC bus. A serial, 2-wire bus used to monitor field replaceable unit (FRU) temperatures and control the system including blade power control.

ID. Identification.

IDB. Interface descriptor block.

IDLE. Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

IEC. International Electrotechnical Commission.

IETF. Internet Engineering Task Force.

information unit (IU). A set of information as defined by either upper-level process protocol definition or upper-lever protocol mapping.

initiator. A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *target.*

in-order delivery (IOD). A parameter that, when set, guarantees that frames are either delivered in order or dropped.

integrated fabric. The fabric created by six switches cabled together and configured to handle traffic as a seamless group.

Internet protocol (IP). In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

inter-switch link (ISL). A Fibre Channel link that connects two switches (a link from the expansion port (E_port) of one switch to the E_port of another).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1204
Doc. 3698

IOD. See *in-order delivery.*

IP. See *internet protocol.*

IPA. Initial process associator.

ISL. See *inter-switch link.*

ISL Trunking. A feature that enables distribution of traffic over the combined bandwidth of up to four inter-switch links (ISLs) (between adjacent switches), while preserving in-order delivery. A set of trunked ISLs is called a trunking group; each port employed in a trunking group is called a trunking port. See also *master port.*

isolated E_port. An expansion port (E_port) that is online but not operational between switches due to overlapping domain ID or nonidentical parameters such as error delay timeout values (E_D_TOVs). See also *expansion port.*

IU. See *information unit.*

K28.5. A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern. See also *comma.*

kernel flash. Flash memory that stores the bootable kernel code and is visible within the memory space of the processor. Data is stored as raw bits.

key pair. In public key cryptography, a pair of keys consisting of a public and private key of an entity. The public key can be publicized, but the private key must be kept secret.

LAN. See *local area network.*

latency. The period of time required to transmit a frame, from the time it is sent until it arrives.

LED. See *light-emitting diode.*

light-emitting diode (LED). A semiconductor chip that gives off visible or infrared light when activated.

link. As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibers. See also *circuit.*

link services. A protocol for link-related services.

LIP. See *loop initialization primitive.*

LM_TOV. See *loop master timeout value.*

local area network (LAN). A computer network located on a user's premises within a limited geographical area. (T)

logical unit number (LUN). An identifier used on a small computer systems interface (SCSI) bus to distinguish among up to eight devices (logical units) with the same SCSI ID.

long wavelength (LWL). A type of fiber optic cabling that is based on 1300 mm lasers and supports link speeds of 1.0625 Gbps. Can also refer to the type of GBIC or SFP. See also *short wavelength.*

loop. A configuration of devices that are connected to the fabric by way of a fabric loop port (FL_port) interface card.

loop circuit. A temporary bidirectional communication path established between loop ports (L_ports).

loop failure. Loss of signal within a loop for any period of time, or loss of synchronization for longer than the timeout value.

loop_ID. A hexadecimal value representing one of the 127 possible arbitrated loop physical address (AL_PA) values in an arbitrated loop.

loop initialization. The logical procedure used by a loop port (L_port) to discover its environment. Can be used to assign arbitrated loop physical address (AL_PA) addresses, detect loop failure, or reset a node.

loop initialization primitive (LIP). The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

looplet. A set of devices connected in a loop to a port that is a member of another loop.

loop master timeout value (LM_TOV). The minimum time that the loop master waits for a loop initialization sequence to return.

loop mode. One of the modes for a loop port (L_port). An L_port is in loop mode when it is in an arbitrated loop and is using loop protocol. An L_port in loop mode can also be in participating mode or nonparticipating mode. See also *loop port*, *fabric mode*, *participating mode*, and *nonparticipating mode.*

loop port (L_port). A node port (NL_port) or fabric port (FL_port) that has arbitrated loop capabilities. An L_port can be either in fabric mode or loop mode. See also *fabric mode*, *loop mode*, *nonparticipating mode*, and *participating mode.*

loop port state machine (LPSM). The logical entity that performs arbitrated loop protocols and defines the behavior of loop ports (L_ports) when they require access to an arbitrated loop.

L_port. See *loop port.*

LPSM. See *loop port state machine.*

LSR. Link state record.

LSU. Link state update.

LUN. See *logical unit number.*

LWL. See *long wavelength.*

MAC. Media access controller.

management information base (MIB). A simple network management protocol (SNMP) structure to help with device management, providing configuration and device information.

master port. As relates to trunking, the port that determines the routing paths for all traffic flowing through the trunking group. One of the ports in the first inter-switch link (ISL) in the trunking group is designated as the master port for that group. See also *ISL Trunking.*

MIB. See *management information base.*

modem serial port. The upper serial port on the control processor card (CP card) of the 2109 Model M12. Can be used to connect the CP card to a modem with a standard 9-pin modem cable. Consists of a DB-9 connector wired as an RS-232 device, and can be connected by serial cable to a data communications equipment (DCE) device. A Hayes-compatible modem or Hayes-emulation is required. The device name is ttyS1. See also *data communications equipment port* and *terminal serial port.*

multicast. The transmission of data from a single source to multiple specified node ports (N_ports), as opposed to all the ports on the network. See also *broadcast* and *unicast.*

multimode. A fiber optic cabling specification that allows up to 500 m (1640.5 ft) between devices.

name server. Frequently used to indicate Simple Name Server. See also *simple name server.*

NEMA. National Electrical Manufacturers Association.

NL_port. See *node loop port.*

NMS. Network Management System.

node. A Fibre Channel device that contains a node port (N_port) or node loop port (NL_port).

node loop port (NL_port). A node port that is loop capable. Used to connect an equipment port to the fabric in a loop configuration through a fabric loop port (FL_port).

node name. The unique identifier for a node, communicated during login and port discovery.

node port (N_port). A node port that is not loop capable. Used to connect an equipment port to the fabric.

nonparticipating mode. A mode in which a loop port (L_port) in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an arbitrated loop physical address (AL_PA) cannot be acquired. See also *participating mode.*

nonvolatile random access memory (NVRAM). Random access memory (storage) that retains its contents after the electrical power to the machine is shut off. A specific part of NVRAM is set aside for use by the system ROS for the boot device list.

N_port. See *node port.*

NVRAM. See *nonvolatile random access memory.*

Nx_port. A node port that can operate as either a node port (N_port) or node loop port (NL_port). See also *node port* and *node loop port.*

operating system (OS). A collection of system programs that control the overall operation of a computer system.

ordered set. A transmission word that uses 8b/10b mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include frame delimiters, primitive signals, and primitive sequences. Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames. See also *frame delimiter*, *primitive signal*, and *primitive sequence.*

OS. See *operating system.*

packet. A set of information transmitted across a network. See also *frame.*

participating mode. A mode in which a loop port (L_port) in a loop has a valid arbitrated loop physical address (AL_PA) and can arbitrate, send frames, and retransmit received transmissions. See also *nonparticipating mode.*

path selection. The selection of a transmission path through the fabric. Switches use the Fibre Channel shortest path first (FSPF) protocol.

PCI. Peripheral control interconnect.

PDU. Power distribution unit.

Performance Monitoring. A feature that provides error and performance information to the administrator and user for use in storage management.

phantom address. An arbitrated loop physical address (AL_PA) value that is assigned to a device that is not physically in the loop. Also known as phantom AL_PA.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1205
Doc. 3698

phantom device. A device that is not physically in an arbitrated loop, but is logically included through the use of a phantom address.

PLDA. See *private loop direct attach.*

PLOGI. See *port login.*

PMC. PCI mezzanine card.

P/N. Part number.

point-to-point. A Fibre Channel topology that employs direct links between each pair of communicating entities.

port cage. The metal casing extending out of the optical port on the switch, and in which the gigabit interface converter (GBIC) or small form-factor pluggable (SFP) can be inserted.

port card. A Fibre Channel card that contains optical or copper port interfaces, and acts like a switch module. See also *16-port card.*

port login (PLOGI). The port-to-port login process by which initiators establish sessions with targets. See also *fabric login.*

port module. A collection of ports in a switch.

port_name. The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST. See *power-on self-test.*

power-on self-test (POST). A series of diagnostics that are automatically run by a device when the power is turned on.

primary FCS switch. Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric. See also *backup FCS switch* and *FCS switch.*

primitive sequence. A part of an ordered set that indicates or initiates port states. See also *ordered set.*

primitive signal. A part of an ordered set that indicates events. See also *ordered set.*

principal switch. The switch that assumes the responsibility to assign domain IDs. The role of principal switch is negotiated after a "build fabric" event.

private device. A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.

private loop. An arbitrated loop that does not include a participating fabric loop port (FL_port).

private loop direct attach (PLDA). A subset of fibre channel standards for the operation of peripheral devices.

private NL_port. A node loop port (NL_port) that communicates only with other private NL_ports in the same loop and does not log into the fabric.

protocol. A defined method and a set of standards for communication.

public device. A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

public loop. An arbitrated loop that includes a participating fabric loop port (FL_port), and can contain both public and private node loop ports (NL_ports).

public NL_port. A node loop port (NL_port) that logs into the fabric, can function within either a public or private loop, and can communicate with either private or public NL_ports.

quad. A group of four adjacent ports that share a common pool of frame buffers.

QuickLoop. (1) A feature that makes it possible to allow private devices within loops to communicate with public and private devices across the fabric through the creation of a larger loop. (2) The arbitrated loop created using this software. A QuickLoop can contain a number of devices or looplets; all devices in the same QuickLoop share a single arbitrated loop physical address (AL_PA) space.

QuickLoop mode. A hardware translative mode that allows private devices to communicate with other private devices across the fabric. See also *hardware translative mode* and *standard translative mode.*

RAID. See *redundant array of independent disks.*

RAM. See *random access memory.*

RAN. Remote Asynchronous Notification.

random access memory (RAM). A temporary storage location in which the central processing unit (CPU) stores and executes its processes.

R_A_TOV. See *resource allocation timeout value.*

read only memory (ROM). Memory in which stored data cannot be changed by the user except under special conditions.

receiver ready (R_RDY). A primitive signal indicating that the port is ready to receive a frame.

reduced instruction set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid processing.

redundant array of independent disks (RAID). A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

registered state change notification (RSCN). A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

remote fabric. A fabric that spans across wide area networks (WANs) by using protocol translation (a process also known as tunneling) such as fibre channel over asynchronous transfer mode (ATM) or fibre channel over Internet protocol (IP).

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server.

Remote Switch. A feature that runs on Fabric operating system (OS) and enables two fabric switches to be connected over an asynchronous transfer mode (ATM) connection. This requires a compatible Fibre Channel to ATM gateway, and can have a distance of up to 10 km (6.214 mi) between each switch and the respective ATM gateway.

request rate. The rate at which requests arrive at a servicing entity. See also *service rate.*

resilient core. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric.

resource allocation timeout value (R_A_TOV). Used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. This value is adjustable in one microsecond increments from 10 - 120 seconds.

resource recover timeout value (RR_TOV). The minimum time a target device in a loop waits after a loop initialization primitive (LIP) before logging out a small computer systems interface (SCSI) initiator. See also *error detect timeout value* and *resource allocation timeout value.*

RISC. See *reduced instruction set computer.*

RLS probing. Read link status of the arbitrated loop physical addresses (AL_PAs).

ro. Read only.

ROM. See *read only memory.*

route. As applies to a fabric, the communication path between two switches. Can also apply to the specific path taken by an individual frame, from source to destination. See also *Fibre Channel shortest path first.*

routing. The assignment of frames to specific switch ports, according to frame destination.

RPC. See *remote procedure call.*

R_RDY. See *receiver ready.*

RR_TOV. See *resource recovery timeout value.*

RS-232 port. A port that conforms to a set of Electrical Industries Association (EIA) standards. Used to connect data terminal equipment (DTE) and data communications equipment (DCE) devices for communication between components, terminals, and modems. See also *DB-9 connector, DCE port,* and *DTE port.*

RSCN. See *registered state change notification.*

RSH. Remote shell.

RTC. Real time clock.

rw. Read-write.

SAN. See *storage area network.*

SAN island. A group of storage devices and servers connected to switches in a fabric.

SC. Standard connector.

SCSI. See *small computer systems interface.*

SCSI Enclosure Services (SES). A subset of the small computer systems interface (SCSI) protocol used to monitor temperature, power, and fan status for enclosure devices.

SDRAM. See *synchronous dynamic random access memory.*

Secure Fabric OS. An optionally-licensed software product that runs on top of the Fabric OS and provides customizable security restrictions through local and remote management channels on a switch.

secure sockets layer (SSL). A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

sequence. A group of related frames transmitted in the same direction between two node ports (N_ports).

SERDES. Serializer/deserializer.

service rate. The rate at which an entity can service requests. See also *request rate.*

SES. See *SCSI Enclosure Services.*

SFP. See *small form-factor pluggable.*

short wavelength (SWL). A type of fiber optic cabling that is based on 850 mm lasers and supports 1.0625 Gbps link speeds. Can also refer to the type of gigabit

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1206
Doc. 3698

interface converter (GBIC) or small form-factor pluggable (SFP). See also *long wavelength*.

SID. The 3-byte source ID of the originator device, in the 0xDomainAreaALPA format.

SID-DID. Source identifier-destination identifier.

SIMMS. Single in-line modules.

simple name server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Can also be referred to as directory service. See also *Fibre Channel service*.

simple network management protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

single mode. The fiber optic cabling standard that corresponds to distances of up to 10 km (6.214 mi) between devices.

small computer systems interface (SCSI). A parallel bus architecture and a protocol for transmitting large data blocks up to a distance of 15 - 25 m (49 - 82 ft).

small form-factor pluggable (SFP). An optical transceiver used to convert signals between optical fiber cables and switches.

SMI. Special memory interface.

SNIA. Storage Network Industry Association.

SNMP. See *simple network management protocol*.

SNMPv1. The original standard for SNMP, now labeled v1.

SNS. See *simple name server*.

SOF. Start-of-frame.

SSL. See *secure sockets layer*.

standard translative mode. A hardware translative mode that allows public devices to communicate with private devices across the fabric. See also *hardware translative mode* and *QuickLoop mode*.

storage area network (SAN). A network of systems and storage devices that communicate using Fibre Channel protocols. See also *fabric*.

subordinate switch. All switches in the fabric other than the principal switch. See also *principal switch*.

switch. Hardware that routes frames according to Fibre Channel protocol and is controlled by software.

switch name. The arbitrary name assigned to a switch.

switch port. A port on a switch. Switch ports can be expansion ports (E_ports), fabric ports (F_ports), or fabric loop ports (FL_ports).

SWL. See *short wavelength*.

synchronous dynamic random access memory (SDRAM). The main memory for the switch. Used for volatile storage during switch operation.

Tachyon. A type of host bus adapter.

target. A storage device on a Fibre Channel network. See also *initiator*.

TCP. See *transmission control protocol*.

tenancy. The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

terminal serial port. The lower serial port on the control processor card (CP card) of the 2109 Model M12. This port sends switch information messages and can receive commands. Can be used to connect the CP card to a computer terminal. Has an RS-232 connector wired as a data terminal equipment (DTE) device, and can be connected by serial cable to a data communications equipment (DCE) device. The connector pins 2 and 3 are swapped so that a straight-through cable can be used to connect to a terminal. The device name is ttyS0. Can also be referred to as the console port. See also *DCE port, DTE port,* and *modem serial port*.

throughput. The rate of data flow achieved within a cable, link, or system. Usually measured in bits per second (bps). See also *bandwidth*.

topology. As applies to fibre channel, the configuration of the Fibre Channel network and the resulting communication paths allowed.

translative mode. A mode in which private devices can communicate with public devices across the fabric.

transmission character. A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Control protocol (TCP). A communications protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for Internet protocol.

transmission word. A group of four transmission characters.

trap (SNMP). The message sent by a simple network management protocol (SNMP) agent to inform the SNMP management station of a critical error. See also *simple network management protocol.*

tunneling. A technique for enabling two networks to treat a transport network as though it were a single communication link or local area network (LAN).

Tx. Transmitted.

U. Unit of measure for rack-mounted equipment.

UART. Universal Asynchronous Receiver Transmitter.

UDP. See *user datagram protocol.*

ULP. See *upper-level protocol.*

ULP_TOV. See *upper-level timeout value.*

unicast. The transmission of data from a single source to a single destination. See also *broadcast* and *multicast.*

universal port (U_port). A switch port that can operate as a generic port (G_port), expansion port (E_port), fabric port (F_port), or fabric loop port (FL_port). A port is defined as a U_port when it is not connected or has not yet assumed a specific function in the fabric.

U_port. See *universal port.*

upper-level protocol (ULP). The protocol that runs on top of Fibre Channel. Typical upper-level protocols are small computer system interface (SCSI), Internet protocol (IP), HIPPI, and IPI.

upper-level timeout value (ULP_TOV). The minimum time that a small computer system interface (SCSI) upper-level protocol (ULP) process waits for SCSI status before initiating ULP recovery.

user datagram protocol (UDP). A protocol that runs on top of Internet protocol (IP) and provides port multiplexing for upper-level protocols.

user flash. See *compact flash.*

VC. See *virtual circuit.*

VCCI. Voluntary Control Council for Interference

virtual circuit (VC). A one-way path between node ports (N_ports) that allows fractional bandwidth.

WAN. See *wide area network.*

WDM. Wave division multiplexing.

well-known address. As pertaining to fibre channel, a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan network, and that can use or provide public communications facilities. (T)

workstation. A computer used to access and manage the fabric. Can also be referred to as a management station or host.

worldwide name (WWN). Uniquely identifies a switch on local and global networks.

World Wide Web (WWW). A network of servers that contain programs and files. Many of the files contain hypertext links to other documents available through the network.

WWN. See *worldwide name.*

WWW. See *World Wide Web.*

XLWL. See *extra long wavelength.*

zone. A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone. See also *zoning.*

zone alias. An alias for a set of port numbers or worldwide names (WWNs). Zone aliases can be used to simplify the entry of port numbers and WWNs. For example, "host" could be used as an alias for a WWN of 110:00:00:60:69:00:00:8a.

zone configuration. A set of zones designated as belonging to the same zone configuration. When a zone configuration is in effect, all valid zones in that configuration are also in effect.

zone member. A port, node, worldwide name (WWN), or alias, which is part of a zone.

zone scheme. The level of zoning granularity selected. For example, zoning can be done by switch or port, worldwide name (WWN), arbitrated loop physical address (AL_PA), or a mixture. See also *zone configuration.*

zone set. See *zone configuration.*

Zoning. A feature that runs on Fabric operating system (OS) and allows partitioning of the fabric into logical groupings of devices. Devices in a zone can only access and be accessed by devices in the same zone. See also *zone.*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1207
Doc. 3698

Index

Numerics

16-port card
  description 28
  LEDs 32
  removing 70
  replacing 74
  specifications 100
2109 Model C36
  attaching
    concrete floor 10
    concrete floor beneath a raised floor 12
    front door 16
    mounting plates 15
    stabilizers 9
  checking
    customer's ac power source 16
    power distribution unit 17
  connecting the switch and device cables 18
  installing 7
  leveling 8
  positioning 7
  powering on the cabinet 18
  regulatory specifications 107
  with Model M12 library xxiii
2109 Model M12
  16-port card 28
  ac power input connectors and ac power switches 30
  blower assembly
    description 30
    side 4
  cable management items 31
  circuit breaker 30
  components 27, 99
  control processor cards 28
  diagnostic tests 43
  features 1
  field replaceable units (FRUs) 43
  installing
    additional model 51
    modems 45, 47
  interpreting
    LED activity 32
    POST 42
  LEDs
    16-port card 32
    blower assembly 40
    CP card 35
    power supply 38
    WWN card 31, 41
  maintenance commands and environmental status 44
  management interfaces 5
  managing and monitoring 4
  operating 27
  overview 1
  parts 117
2109 Model M12 *(continued)*
  port side 3
  power supplies 30
  removing additional model 51
  setting up a remote modem system 46
  standard shipment 53
  starting and configuring 19
  turning on and off 27
  unpacking 53
  verifying modem installation 48
24-inch load plate
  part number 52
  using 60

A

about this document xxiii
ac grounding check xviii
ac power
  external cords 17
  how to remove xiv
  input connectors 30
  switches 30
ac power distribution unit
  power-off procedure 70
  power-on procedure 69
  removing 95
  replacing 95
accessory kit 53
activity LED, interpreting 32
address of IBM xxv
Advanced Security feature 2
Agency Certification label xii
assembly, blower
  description 30
  LEDs 40
  side of chassis 4
attaching
  cabinet to concrete floor 10, 12
  front door 16
  mounting plate 15
  stabilizer 9
attention notices xi
audience xxiii

B

battery
  CP card 99
  CP card, replacing 86
  notice, caution xxii
  specifications 101
bezel
  description 31
  LEDs 41
blank
  fillers 111

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1208
Doc. 3698

blank *(continued)*
planning worksheets 119
blower assembly
description 30
LEDs 40
removing 90
replacing 90
side of chassis 4
time required 90
brace, earthquake 110
brackets, installing 55
bridge tool
alignment label, inspecting xviii
inspecting the label xviii
ordering 52
part number 52
purpose of 52
returning 52
using 60
Brocade
documents xxiii
IBM product and model number matrix xxiv

C

cabinet
attaching to a concrete floor 10
attaching to concrete floor 12
door, removing and replacing 96
external check xiii
inspection xi
installing the 2109 Model M12 55
leveling 8
parts 115
positioning 7
power on 18
power-off procedure 70
power-on procedure 69
relocating 97
removing a 2109 Model M12 from 65
removing and replacing the PDU 94
safety label checks xii
service 69
cable management
items 31
tray
removing 91
replacing 92
cables
alignment 25
guides 32
recommendations for managing 75
card
16-port card 28
control processor 28
WWN 31
caution notices
battery xxii
definition xi
chassis
port side 3
chassis *(continued)*
providing initial power 19
chassis door
removing 54, 96
replacing 96
check
ac grounding xviii
ac power source of the customer 16
ground xviii
machine, external xiv
machine, internal xiv
PDU 17
safety label xv
Chinese Class A compliance statement 124
circuit breaker 30
Class 1 laser product xxi
comments, how to send xxv
components
2109 Model M12 99
switch 27
concrete floor cabinet attachment 10, 12
conducting
external machine checks xiv
internal machine checks xiv
safety inspections xi
configuration
2109 Model M12 19
parameters 21
switch 21
Confirming, a failed CP card 76
connect the switch and device cables 18
control processor card
description 28
determining the status 29
LEDs 35
removing 79
replacing 81
specifications 101
cords, power 113
covers, parts 109
CP card battery, replacing 86
customer ac power source 16

D

danger notices xi
device cables, connecting 18
diagnostic tests 43
digital meter xviii
dimensions, physical 99
director of licensing, address 123
disposal, product xxii
Do Not Operate tag 16
document, about this xxiii
door
cabinet
removing 96
replacing 97
chassis
removing 54, 96
replacing 96

90.866

E

earthquake brace, parts 110
edition notice ii
electrical safety 69
electronic emission statements 124
environmental
  notices and statements xxi
  requirements 104
  status and maintenance commands 44
Ethernet port 29
European Community compliance statement 125
Extended Fabrics 2
external
  ac power cords 17
  cabinet checks xiii
  machine checks
    battery notice caution xxii
    how to conduct xiv

F

Fabric Manager 2
facility specifications 103
factory, configuration 18
FCC
  emission limits 124
  rules 124
  statement 124
  unauthorized changes or modifications 124
FDA 21 CFR 1040.10 and 1040.11 xxi
features
  Advanced Zoning 2
  Fabric Watch 2
  ISL Trunking 2
  Performance Monitoring 2
  software
    Advanced Security 2
    Extended Fabrics 2
    Fabric Manager 2
    Remote Switch 2
  Web Tools 2
features, 2109 Model M12 1
Federal Communications Commission (FCC)
 statement 124
Fibre Channel Association Web site xxiv
Fibre Channel port specifications 102
field replaceable units (FRUs) 43
filler panel
  16-port card, removing 70
  16-port card, replacing 74
  CP card, removing 79
  CP card, replacing 81
  power supply, removing 87
  power supply, replacing 89
fire suppression systems xxii
form
  non-IBM alteration attachment survey xiv
  reader comment, how to send xxv
front door attachment 16
fruinfoset command 97
fusing caution label xvi

G

general specifications of the 2109 Model C36 with
 Model M12 105
genie tool and load plate label, inspecting xviii
Germany compliance statement 125
getting
  help xxiv
  software updates xxiv
ground
  attachment plug 17
  checking ac xviii
  checks xviii
  lug xviii
guidelines
  safety 51

H

heavy load label xvi
help, getting xxiv
high
  leakage current label xii
  voltage, ac 17
High-availability feature 1
how to send your comments xxv

I

IBM
  address xxv
  notices 123
  trademarks 124
IBM product and model number matrix xxiv
IEC 825-1 xxi
in-band management method 4
Industry Canada compliance statement 124
information, parts 109
inlet, power requirements 103
inspection
  bridge tool xviii
  Model 2109 M12 switch xiv
  safety, cabinet xi
  safety, conducting xi
installation considerations and safety guidelines 51
installing
  2109 Model C36 7
  2109 Model M12 in the cabinet 55, 60
  additional 2109 Model M12 51
  brackets 55
  modems 45, 47
intellectual property 123
interference, radios and televisions 124
internal machine checks xiv
interpreting
  LED activity 32
  POST 42
items
  2109 Model M12 standard shipment 53

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1209
Doc. 3698

items *(continued)*
cable management 31
needed
configure and connect the 2109 Model M12 20
required
remove a blower assembly 90
remove a cable management tray 91

J

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 126

K

Korean Government Ministry of Communication (MOC) statement 126

L

label
Agency Certification xii
bridge tool alignment xviii
check, safety xv
fusing caution xvi
Genie tool and load plate xx
heavy load xvi
high leakage current danger xii
linecord caution xv
pinch point xxi
power supply cord caution xii
power supply cover caution xvi
SFP xvii
tilt warning xx
laser safety xxi
LEDs
16-port card 32
activity, interpreting 32
blower assembly 40
control processor card 35
patterns
16-port card 33
blower assembly 40
CP card 37
power supply 39
power supply 38
WWN card and bezel 41
leveling
cabinet 8, 14
feet 8, 113
license
for patents 123
lift tool
arbocrate (shipping container) 53
ordering procedure 52
part number 52
United States ordering procedure 52
unpacking, assembly and repacking 55
using 60, 65
World trade ordering procedure 52
linecord caution label xv
lug, ground xviii

M

machine checks
external xiv
internal xiv
maintaining the 2109 Model M12 43
maintenance commands and environmental status 44
managing
cable items 31
cables, recommendations 75
materials, recyclable xxii
memory specifications 101
meter, digital xviii
modem
installation, verifying 48
installing 45, 47
serial port port pinouts 102
serial port specifications 102
setup 46
monitoring and managing the switch 4
mounting plate attachment 15

N

needed items, to configure and connect the 2109 Model M12 20
non-IBM alteration attachment survey form xiv
notices
caution, battery xxii
environmental xi, xxi
IBM 123
safety xi, 69

O

operating the 2109 Model M12 27
optical port terminators xxi
ordering the lift tool and the 24–inch load plate 52
out-of-band management method 4
overview of the 2109 Model M12 1

P

parameters
configuration 21
modem for Windows 95, 98, 2000, ME or NT, or TERM in a UNIX environment 47
part number
24-inch load plate 52
lift tool 52
parts
2109 Model M12 117
blank fillers 111
covers 109
earthquake brace 110
information 109
leveling feet 113
PDU 116

parts *(continued)*
power cords 113
stabilizers 112
supplied with the 14U mount kit 115
patents 123
PDU
check 17
parts 116
power-off procedure 70
power-on procedure 69
removing 95
replacing 95
physical dimensions 99
pinch point label, inspecting xviii
pinouts
modem serial port 102
terminal serial port 101
planning worksheet 119
port
configuration worksheet 120
Ethernet 29
modem serial 29
side of chassis 3
switch 99
terminal serial 29
terminal serial, specifications 101
position the cabinet 7
POST
interpreting 42
restarting 107
specifications 107
power
cords
external 17
list of 113
removing xiv
source check 16
specifications 103
to the chassis 19
power distribution unit (PDU)
check 17
parts 116
power-off procedure 70
power-on procedure 69
removing 95
replacing 95
power supply
cord caution label xii
cover caution label xvi
description 30
LEDs 38
removing 87
replacing 89
turning on and off 27
power-off procedure
PDU 70
power-on procedure
cabinet 69
PDU 69
product
disposal xxii
product *(continued)*
recycling xxii
specifications 99, 100
proper grounding xviii
providing initial power to the chassis 19
publications
2109 Model C36 with Model M12 library xxiii
Web sites xxiv

R

radio interference 124
reader comment form processing xxv
recommendations for managing cables 75
Recording critical switch information 77
recycling products xxii
reference information for the fruinfoset command 97
regulatory specifications 106
related documents xxiii
relocating the cabinet 97
remote modem setup 46
Remote Switch 2
removing
16-port card 70
16-port card filler panel 70
2109 Model M12 from the cabinet 65
ac power xiv
blower assembly 90
cabinet door 96
cable management tray 91
chassis door 54, 96
CP card 79
filler panel 79, 87
PDU 94
power supply or filler panel 87
removing and replacing
16-port card 70
16-port card filler panel 70
blower assembly 89
cable management tray 91
chassis door 95
CP card or filler panel 75
front and rear doors 96
PDU 94
power supply or filler panel 86
WWN card 93
replacing
16-port card 74
16-port card filler panel 74
blower assembly 90
cabinet door 97
cable management tray 92
chassis door 96
CP card battery 86
CP card or filler panel 81
filler panel 81, 89
PDU 95
power supply or filler panel 89
required items
to remove a blower assembly 90
requirements, environmental 104

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1210
Doc. 3698

restarting the switch 107
restrictions, usage xxi
running a POST 42

S

safety
cabinet label check xii
electrical 69
external cabinet check xiii
external machine checks xiv
guidelines 51
inspection, how to conduct xi
internal machine checks xiv
label check xv
laser xi, xxi
notices xi, 69
product disposal xxii
sending your comments xxv
servicing the cabinet 69
setting up a remote modem system 46
SFP label xvii
software
features
Advanced Security 2
Advanced Zoning 2
Extended Fabrics 2
Fabric Manager 2
Fabric Watch 2
ISL Trunking 2
Performance Monitoring 2
Remote Switch 2
Web Tools 2
getting updates xxiv
specifications
16-port card 100
battery 101
facility 103
Fibre Channel port 102
general 105
memory 101
modem serial port 102
POST 107
power 103
product 100
regulatory 106
restarting 107
terminal serial port 101
SPF, inserting 25
stabilizer
attaching 9
parts 112
standard shipment items 53
starting and configuring the 2109 Model M12 19
statements
Chinese Class A compliance 124
electronic emission 124
European Community compliance 125
Federal Communications Commission 124
Germany compliance 125
Industry Canada compliance 124
statements *(continued)*
Japanese Voluntary Control Council for Interference (VCCI) class 1 126
Korean Government Ministry of Communication (MOC) 126
Taiwan class A compliance 126
switch
components 27, 99
configuring 19, 21
connecting 18
inspecting the Model 2109 M12 xiv
managing 4
operating 27
ports 99
POST, interpreting 42
restarting 42
specifications
facility 103
general 105
memory 101
modem serial port 102
power 103
regulatory 106
terminal serial port 101
turning on and off 27
worksheets
planning 119
port configuration 120
zone configuration 122
zone definition 121
systems, fire suppression xxii

T

tag, Do Not Operate tag 16
Taiwan class A compliance statement 126
take-back program, product xxii
terminal
serial port specifications 101
terminators for optical ports xxi
tests, diagnostic 43
tie wraps 32
tilt warning label, inspecting xviii
time required to install the 2109 Model M12 in the cabinet 55
time required to remove and replace
16-port card or filler panel 70
blower assembly 90
cable management tray 91
chassis door 95
CP card or filler panel 76
power supply or filler panel 87
tools required to install the 2109 Model M12 in the cabinet 55
trademarks 124
turning on and off the 2109 Model M12 27

U

United States ordering procedure for the lift tool and the 24-inch load plate 52

units , field replaceable 43
unpacking the 2109 Model M12 53
updates, getting software xxiv
usage restrictions xxi
using the lift tool, the 24-inch load plate, and the bridge tool 60

V

verifying
if the WWN card needs replacing 93
modem installation 48
the operation of the new CP card 82
voltage level at power source xviii

W

Web sites xxiv
weight, component 99
who should read this document xxiii
worksheets
blank 119
planning 119
port configuration 120
zone configuration 122
zone definition 121
World trade ordering procedure for the lift tool and the 24-inch load plate 52
WWN card
and bezel 31
and bezel LEDs 41
restarting the switch 31

Z

zone
configuration worksheet 122
definition worksheet 121

RQS-nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1211
Doc. 3698

Readers' comments—we would like to hear from you

IBM TotalStorage SAN Cabinet
2109 Model C36 with Model M12
Installation and Service Guide

Publication No. GC26-7467-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1212
Doc. 3698

Readers' Comments — We'd Like to Hear from You
GC26-7467-03

IBM®

Cut or Fo
Along Lin

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
RCF Processing Department
M86/050-3
5600 Cottle Road
San Jose, CA 95193-0001

Fold and Tape | **Please do not staple** | Fold and Tape

GC26-7467-03

Cut or Fold
Along Line

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1213
Nº Doc. 3698

Spine information:

IBM

IBM TotalStorage SAN Cabinet

IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12: Installation and Service Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1214
Doc 3698

10.858

10.857

Manual 04

Interoperability Matrix

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1215
Doc. 3698

10.856

IBM TotalStorage™ Enterprise Storage Server™

Interoperability Matrix

June 27, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1216
Doc. 3698

© Copyright International Business Machines Corporation 1999, 2002, 2003. All rights reserved.

The information provided in this document is provide "AS IS" without warranty of any kind, including any warranty of merchantability, fitness for a particular purpose, interoperability or compatibility. IBM's products are warranted in accordance with the agreements under which they are provided.

Unless otherwise specified, the product manufacturer, supplier, or publisher of non-IBM products provides warranty, service, and support directly to you. IBM makes no representations or warranties regarding non-IBM products.

The inclusion of an IBM or non-IBM product on an interoperability list is not a guarantee that it will work with the designated IBM storage product. In addition, not all software and hardware combinations created from compatible components will necessarily function properly together. The following list includes products developed or distributed by companies other than IBM. IBM does not provide service or support for the non-IBM products listed, but does not prohibit them from being used together with IBM's storage products. During problem debug and resolution, IBM may require that hardware or software additions be removed from the IBM product to provide problem determination and resolution on the IBM-supplied hardware/ software. For support issues regarding non-IBM products, please contact the manufacturer of the product directly. IBM does not warrant either functionality or problem resolution of any non-IBM products.

This information could include technical inaccuracies or typographical errors. IBM does not assume any liability for damages caused by such errors as this information is provided for convenience only; the reader should confirm any information contained herein with the associated vendor.

Changes are periodically made to the content of the document. These changes will be incorporated in new editions of the document. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this document at anytime without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX	IBM logo	S/390
AS/400	Micro Channel	S/390 Parallel Enterprise Server
DYNIX	Multiprise	SP
DYNIX/ptx	Netfinity	TotalStorage
e (logo)	NUMA-Q	Versatile Storage Server
Enterprise Storage Server	OS/390	VM/ESA
ESCON	OS/400	VSE/ESA
ES/9000	PTX	xSeries
FICON	pSeries	z/OS
FlashCopy	Redbooks	zSeries
IBM	RS/6000	z/VM

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

CONTENTS

Introduction 2
ESS Interoperability Summary 3
Configuration Planning 4
ESS Copy Services 6
Data General Servers 9
Hewlett-Packard Servers – HP-UX 11
Hewlett-Packard Servers – OpenVMS 13
Hewlett-Packard Servers – Tru64 UNIX 15
IBM iSeries and AS/400 Servers 17
IBM NUMA-Q Servers 19
IBM pSeries and RS/6000 Servers 21
IBM RS/6000 SP Servers 25
IBM zSeries and S/390 Servers 29
Intel-based Servers – Linux 34
Intel-based Servers – NetWare 36
Intel-based Servers – Windows 39
SGI Servers 42
Sun Servers 44
Network Attached Storage (NAS) 47
Appendix A: ESS Host Adapters and Cables 49
Appendix B: Host Adapter Products 50
Appendix C: SAN Fabric Products 53
Appendix D: Revision History 54

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1217 Page
Doc. 3698

About this Document

This document lists interoperable environments and configurations for IBM TotalStorage Enterprise Storage Server (ESS).

The document is for informational and planning purposes only and may change at anytime. This version supersedes and replaces all previous versions. The latest version of this document is available at:
http://www.ibm.com/storage/hardsoft/products/ess/supserver.htm

Not all combinations created from interoperable components are supported, nor will they necessarily function properly together. The customer is responsible for confirming that a specific configuration (i.e. server model, operating system level, host adapter, and fabric product combination) is a valid and supported configuration by each of the vendors whose products are included in the configuration.

This document is not intended to be the sole resource for configuration information, requirements, and prerequisites. Refer to ESS publications, vendor documentation, or your IBM Sales Representative or IBM Business Partner for additional information.

End-of-Service / End-of-Support

Throughout this document, this symbol – @ – indicates that the product vendor has announced that they no longer provide support for the product. If problems are encountered with existing installations, you may be required to update your configura to a supported level before problem determination can take place.

Request for Price Quotations (RPQ)

If a desired configuration is not represented in this document, a RPQ should be submitted to IBM to request approval. To submit a RPQ, contact your local IBM Storage Specialist or Business Partner.

Examples of configurations supported via RPQ are available at:
http://www.storage.ibm.com/hardsoft/products/ess/additional_config.html

What's New

This version is dated June 27, 2003 and has been updated as noted below. It replaces the version dated May 13, 2003. Unless stated otherwise, these items require ESS LIC level 2.2.0, or later.

Servers
- IBM BladeCenter (Intel(Linux and Windows))
- IBM TotalStorage SAN Volume Controller
- pSeries 615 Models 6C3 and 6E3

Operating Systems, Path Management, and Clustering
- UnitedLinux 1.0 (iSeries and pSeries): SuSE Enterprise Server 8
- Windows 2003 SDD
- zSeries: Added End-of-Service/End-of-Support notation for zSeries O/S levels
- zSeries Fibre Channel Protocol
- zSeries: z/VM Version 4 Release 3

Host Adapters
- Emulex LP9402DC and LP 9802: Added availability date for support on NetWare
- IBM FC 6239 (pSeries)
- SGI PCX-FC-2OPT-B

SAN Fabric
- IBM RS/6000: Cisco MDS 9216 and 9509

ESS INTEROPERABILITY SUMMARY

For convenience, the following tables summarize the interoperable environments and configurations for the ESS. Refer to the individual server pages for additional information, including prerequisites and limitations.

Table 1: Open Systems

	ESS Model 800	ESS Models F10 and F20	ESS Models E10 and E20	Fibre Channel	SCSI	Clustering (Fibre Channel)	Clustering (SCSI)	Boot device support	Subsystem Device Driver (SDD)	ESS Application Program Interface (ESS API)	ESS Command Line Interface (ESS CLI)	Copy Services Command Line Interface (CS CLI)
Data General (DG/UX)		✓	✓		✓							
Hewlett-Packard (HP-UX)	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
Hewlett-Packard AlphaServer (OpenVMS)	✓	✓	✓	✓	✓	✓	✓					✓
Hewlett-Packard AlphaServer (Tru64 UNIX)	✓	✓	✓	✓	✓	✓	✓	✓				✓
IBM iSeries and AS/400 (OS/400)	✓	✓	✓	✓	✓							
IBM iSeries and AS/400 (Linux)	✓			✓								
IBM pSeries, RS/6000, and RS/6000 SP (AIX)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IBM NUMA-Q (DYNIX/ptx)	✓	✓	✓	✓		✓						✓
Intel Servers (Linux)	✓	✓		✓					✓	✓	✓	✓
Intel Servers (NetWare)	✓	✓	✓	✓	✓	✓	✓		✓			✓
Intel Servers (Windows)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGI Origin Servers (IRIX)	✓	✓		✓								
Sun (Solaris)	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓

Table 2: IBM zSeries and S/390

	z/OS and OS/390	z/VM and VM/ESA	VSE/ESA	Transaction Processing Facility (TPF)	Linux for S/390
ESS Model 800	✓	✓	✓	✓	✓
ESS Models F10 and F20	✓	✓	✓	✓	✓
ESS Models E10 and E20	✓	✓	✓	✓	✓
FICON	✓	✓	✓	✓	✓
ESCON	✓	✓	✓	✓	✓

10.852
ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1218
Doc 3698

ESS Technical Support Home Page

The ESS Technical Support Home Page contains links to publications, documentation, downloads, utilities, and other resources.

http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/2105

ESS Licensed Internal Code (LIC)

This document contains references to minimum ESS LIC levels. In many cases, the minimum level listed does not represent the latest available LIC level.

Customers are encouraged to keep their ESS at the latest LIC level to take advantage of quality, reliability, and serviceability enhancements and to receive problem determination and fix support.

ESS LIC level 1.5.2 or later, is the currently recommended level.

Host Systems Attachment Guide

The *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* should be referenced to obtain detailed information on attaching servers to the ESS.

Host Adapters

This document contains only limited information regarding host adapter driver levels and other prerequisites. Host adapter firmware, driver, and fix level information is documented in the ESS Fibre Channel Host Bus Adapter (HBA) Support Matrix. This matrix can be found at:

http://ssddom02.storage.ibm.com/hba/hba_support.pdf

Additionally, review host adapter vendor documentation and web pages to obtain information regarding host adapter configuration planning, hardware and software requirements, driver levels, and release notes.

Emulex: http://www.emulex.com/ts/dds.html

JNI: http://www.jni.com/OEM/oem.cfm?ID=4

QLogic: http://www.qlogic.com/support/oem_detail_all.asp?oemid=22

SAN Fabric Products

Fabric product vendor documentation and web pages should be reviewed to obtain information regarding configuration planning, hardware and software requirements, firmware and driver levels, and release notes.

IBM: www.ibm.com/storage/ibmsan/products/sanfabric.html

INRANGE: www.inrange.com/ibm/

McDATA: www.mcdata.com/ibm/

Cisco: www.cisco.com/go/ibm/storage

SAN Volume Controller

The IBM SAN Volume Controller (IBM 2145 Model 4F2) is supported with the ESS Models F10, F20, and 800, and requires ESS LIC level 2.2.0, or later. Refer to the following web page for specific interoperability information on the SAN Volume Controller:

http://www.ibm.com/storage/support/2145

IBM SAN Data Gateway (SDG)

The SAN Data Gateway (IBM 2108 Model G07) is supported with the ESS Models E10, E20, F10, and F20 for legacy installations only. These installations are encouraged to migrate to native ESS Fibre Channel support.

The ESS Model 800 is not interoperable with the SDG.

Subsystem Device Driver (SDD)

The SDD provides load balancing and enhanced data availability capability in configurations with more than one I/O path between the host server and the ESS. Load balancing can reduce or eliminate I/O bottlenecks that occur when many I/O operations are directed to common devices via the same I/O path. SDD also helps eliminate a potential single point of failure by automatically rerouting I/O operations when a path failure occurs, thereby supporting enhanced data availability capability. The SDD is provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites.

Refer to the *IBM TotalStorage Enterprise Storage Server Subsystem Device Driver User's Guide* for additional information.

Additional SDD information is also available at:

http://www.ibm.com/storage/support/techsup/swtechsup.nsf/support/sddupdates

ESS Application Program Interface (ESS API)

The ESS API can help simplify ESS administration and reduce the total cost of ownership by enabling ESS LUN management activities through implementation of the Storage Management Initiative Specification (SMIS), "Bluefin", as defined by the Storage Networking Industry Association (SNIA). It is implemented through the IBM TotalStorage Common Information Model Agent (CIM Agent) for the ESS, a middleware application that provides a CIM-compliant interface. The ESS API and CIM Agent are provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites. While the CIM Agent is available for only selected operating system environments, it can be used to manage all LUNs within an ESS.

Refer to IBM TotalStorage Common Information Model Agent for the Enterprise Storage Server: Installation and Configuration Guide for additional information.

ESS Command Line Interface (ESS CLI)

The ESS CLI provides an alternate method to perform ESS logical configuration and storage management functions. With the ESS CLI, routine configuration and management tasks can now be automated through their incorporation into scripts and applications, helping to simplify ESS administration and thereby reducing the total cost of ownership. The ESS CLI is provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites. While the ESS CLI is available for only selected operating system environments, it can be used to manage all LUNs within an ESS.

Refer to *IBM TotalStorage Enterprise Storage Server Command Line Interfaces User's Guide* for additional information.

Copy Services Command Line Interface (CS CLI)

The CS CLI enables open systems hosts to invoke and manage FlashCopy and PPRC functions through batch processes and scripts. It provides commands to query the status of ESS volumes and to execute copy services tasks that were previously created using the IBM TotalStorage Enterprise Storage Server Specialist. The CS CLI is provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites.

Refer to *IBM TotalStorage Enterprise Storage Server Command Line Interfaces User's Guide* for additional information.

Additional CS CLI information is also available at:

http://ssddom02.storage.ibm.com/disk/ess/copyservices.html

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1219
Doc 3698

FlashCopy

FlashCopy provides a point-in-time copy capability for data on the ESS. FlashCopy is designed to create a physical point-in-time copy of the data, with minimal interruption to applications, and makes it possible to access both the source and target copies immediately. FlashCopy is an optional feature on the ESS.

Extended Remote Copy (XRC)

XRC is a combined hardware and software business continuance solution for the zSeries and S/390 environments designed to provide asynchronous mirroring between two ESSs at global distances. XRC is an optional feature on the ESS.

Peer-to-Peer Remote Copy (PPRC)

PPRC is a hardware-based business continuance solution designed to provide real-time mirroring of logical volumes within an ESS or to another ESS. PPRC is an optional feature on the ESS.

IBM supports the use of PPRC in the following modes. Refer to Table 3 for ESS model support and LIC prerequisites.

PPRC Synchronous Mode

PPRC synchronous mode can be used for real-time data mirroring. In this mode, updates made on the primary ESS (local site) are synchronously shadowed to a secondary ESS (remote site).

Since this is a synchronous operation, the distance between the primary and secondary ESS will affect the application response time. Therefore, when operating in this mode, PPRC has a standard maximum supported distance of 103 km between the primary and secondary ESS.

PPRC synchronous mode can be used at distances beyond 103 km with prior approval from IBM. Approval can be requested by submitting a Request for Price Quotation (RPQ). The RPQ should include information on distance between sites, the channel extension technology, the type of telecom line, the amount of network bandwidth, the ESS capacity, and a general description of the workload.

Long Distance Data Copy / Migration

PPRC can be used for long distance data copy or migration of static volumes. Static volumes are volumes that do not have write I/O activity while the PPRC copy of data from the primary to the secondary is in progress.

Since there is no write I/O activity while the PPRC data copy is in progress, the distance between the primary and secondary ESS will not affect application response time. Therefore, when operating in this mode, PPRC can be used with much greater distances between the primary and secondary ESS (as compared to PPRC synchronous mode).

PPRC Extended Distance (PPRC-XD)

PPRC-XD is a non-synchronous long distance copy option suitable for data migration and periodic offsite backup.

With a non-synchronous operation, the distance between the primary and secondary ESS will have only a minimal effect on the application response time. Therefore, PPRC-XD can operate at very long distances.

Asynchronous Cascading PPRC

Asynchronous Cascading PPRC can be used to create three-site or two-site long-distance remote copy solutions. With Asynchronous PPRC, the PPRC secondary volume (involved in a PPRC synchronous relationship) can also simultaneously serve as a PPRC primary volume in a PPRC Extended Distance (PPRC-XD) relationship to the remote site.

PPRC Channel Extension, DWDM, and Network Connectivity Options

Distances beyond 103 km will require the use of channel extension technology, and the channel extender vendor will determine the maximum distance supported. The vendor should be contacted for their distance capability, line quality requirements, and WAN attachment capabilities.

IBM supports the use of the following products with PPRC:

- ESCON directors
- Channel extenders
  - CNT UltraNet Storage Director
  - INRANGE 9801 Storage Networking System
- DWDMs (Dense Wave Division Multiplexers)
  - Cisco ONS 15540
  - IBM 2029 Fiber Saver
  - Nortel Networks OPTera Metro 5200
  - Nortel Networks OPTera Metro 5300

Refer to Table 3 for ESS LIC prerequisites. Additionally, the product vendors should also be consulted regarding hardware and software prerequisites when using their products in an ESS PPRC configuration. IBM is not responsible for third-party products.

When using PPRC with channel extenders, IBM supports the use of PPRC over all the network technologies that are currently supported by the channel extender products, including Fibre Channel, Ethernet/IP, ATM-OC3, and T1/T3. Evaluation, qualification, approval, and support of PPRC configurations using channel extender products are the sole responsibility of the channel extender vendor. The vendor should be contacted for their distance capability, line quality requirements, and WAN attachment capabilities.

Table 3: Minimum ESS LIC Levels for PPRC

	PPRC Synchronous Mode	PPRC Long Distance Data Copy / Migration	PPRC-XD	Asynchronous Cascading PPRC
ESS Model 800	2.0.0	2.0.0	2.0.0	2.2.0
ESS Models F10 and F20	1.3.0	1.5.0	1.5.2	2.2.0
ESS Models E10 and E20	1.3.0	Not supported	Not supported	Not supported
CNT UltraNet Storage Director	1.5.2	1.5.2	1.5.2	2.2.0
INRANGE 9801 Storage Networking System	1.3.0	1.5.0	1.5.2	2.2.0
IBM 2029 Fiber Saver	1.3.0	1.5.0	1.5.2	2.2.0
Cisco ONS 15540	1.3.4.41	1.5.0	1.5.2	2.2.0
Nortel Networks OPTera Metro 5200	1.3.0	1.5.0	1.5.2	2.2.0
Nortel Networks OPTera Metro 5300	1.3.4.41	1.5.0	1.5.2	2.2.0

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1220
Doc. 3698

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
AviiON • 4900 • 5000	DG/UX • 4.2	Adaptec • AHA-2944UW • AHA-4944W	N/A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1221
Doc 3698

General notes:

- ESS API – CIM Agent:
  - Not available for DG-UX
- ESS CLI:
  - Not available for DG-UX.
- CS CLI:
  - Not available for DG-UX.
- SDD:
  - Not available for DG-UX.
- Data General servers are not interoperable with the ESS Model 800.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

HP Server
• rp5400 series
• rp7400
 	
HP 9000 Enterprise Servers
• D-Class
• E-Class
• G-Class
• H-Class
• I-Class
• K-Class
• L-Class
• N-Class
• T-Class
• V-Class
• Enterprise Parallel Servers
	HP-UX
	• 10.20
	• 11.00
	  • PVLINKS
	  • MC/Serviceguard 11.05/09 [1]
	• 11i
	  • PVLINKS
	  • MC/Serviceguard 11.12 and 11.13
		Hewlett-Packard
		• A2969A
		• A4107A
		• A4800A
		• A5159A
		• 28696A
			N/A

JD. 845

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

HP Server
• rp5400 series
• rp7400
• rp7410 [2]
• rp8400 [2]
• Superdome [2]
 	
HP 9000 Enterprise Servers
• D-Class
• K-Class
• L-Class
• N-Class
• V-Class
	HP-UX
	• 11.00
	  • PVLINKS
	  • MC/Serviceguard 11.05/09 [1]
	• 11i
	  • PVLINKS
	  • MC/Serviceguard 11.12, 11.13, and 11.14
		Hewlett-Packard
		• A3404A
		• A3591B
		• A5158A
		• A6684A
		• A6685A
		• A6795A [3]
			Cisco [3]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2109 Models F16 and F32 [3]
			• 2109 Model M12 [3]
			• 2109 Models S08 and S16
			• 3534 Model F08 [3]
			
			INRANGE
			• FC/9000-64 [4]
			• FC/9000-128 [4]
			• FC/9000- 256 [5]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [3]
			• Sphereon
			  • 3216 [3]
			  • 3232 [3]
			  • 4500 [3]

[1] MC/Serviceguard 11.05/09 can be used with only the K-Class, L-Class, N-Class, and V-Class servers.

[2] Requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.

[3] Requires ESS LIC level 1.5.2, or later.

[4] Requires ESS LIC level 1.3.2.50, or later.

[5] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1222
Doc. 3698

General notes:

- Fibre channel:
  - Requires ESS LIC level 1.3.0, or later.
- ESS API – CIM Agent:
  - Not available for HP-UX.
- ESS CLI:
  - Available for HP-UX 11.0, or later.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for all levels of HP-UX.
  - HP-UX 11i requires ESS LIC level 1.5.2, or later.
- SDD:
  - Not available for or interoperable with:
    - HP-UX 10.20.
    - HP-UX 11 32-bit.
    - HP-UX 11i SCSI configurations.
    - MC/Serviceguard
  - HP-UX 11i requires ESS LIC level 1.5.2, or later.
  - Multi-path support is natively available in HP-UX (PVLINKS).
- The following items are not interoperable with the ESS Model 800:
  - Servers:
    - T-Class.
  - Operating systems:
    - HP-UX 10.20.
  - Host adapters:
    - HP A3404A and HP A3591B.
- The following items are not interoperable with ESS Models E10 and E20:
  - ESS CLI.
  - Servers:
    - rp5400, rp7400, rp7410, rp8400, and Superdome.
  - Host adapters:
    - HP A6795A
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
AlphaServer • 800 • 1200 • 2100 • 4000, 4000A • 4100 • 8200, 8400 • DS10, DS20, DS20E • ES40 • GS60, GS60E, GS140	OpenVMS • 6.2-1 H3 • 7.1-2 • 7.2-1, 7.2-2 [7] • 7.3	StorageWorks • KZPBA-CB	N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support
AlphaServer • 800 • 1200 • 4000, 4000A • 4100 • 8200, 8400 • DS10, DS20, DS20E • ES40 • GS60, GS60E, GS140 • GS80, GS160, GS320	OpenVMS • 7.2-2 • 7.3 • 7.3-1 [8]	StorageWorks • KGPSA-CA • KGPSA-DA [8]	IBM • 2109 Model F16 • 2109 Models S08 and S16 • 3435 Model F08

[7] Requires ESS LIC level 1.5.2, or later.

[8] Requires ESS LIC level 2.2.0, or later.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1223
Doc. 3698

General notes:

- Fibre channel:
  - Requires ESS LIC level 2.1.0, or later.
  - Requires ESS Fibre Channel Host Adapter feature #3021, 3023, #3024, or #3025.
  - Not available for the ESS Models E10 and E20.
- Copy services:
  - Requires ESS LIC level 1.5.2, or later.
- ESS API – CIM Agent:
  - Not Available for OpenVMS.
- ESS CLI:
  - Not available for OpenVMS.
- CS CLI:
  - Available for OpenVMS 7.3, or later.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- SDD:
  - Not available for OpenVMS.

- The following items are not interoperable with the ESS Model 800:
  - Operating systems:
    - Open VMS 6.2.

- The following items are not interoperable with the ESS Models E10 and E20:
  - Fibre channel.
  - Copy services.

10.841

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

AlphaServer
• 800
• 1200
• 2100
• 4000, 4000A
• 4100
• 8200, 8400
• DS10, DS20, DS20E
• ES40
• GS60, GS60E, GS140
	Tru64 UNIX
	• 4.0D, 4.0E
	• 4.0F, 4.0G
	  • ASE 1.6
	• 5.0A
	  • TruCluster 5.0A
	• 5.1
	  • TruCluster 5.1
	• 5.1A [1]
	  • TruCluster 5.1A
		StorageWorks
		• KZPBA-CB
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

AlphaServer
• 800
• 1200
• 2100
• 4000, 4000A
• 4100
• 8200, 8400
• DS10, DS20, DS20E
• ES40
• GS60, GS60E, GS140
• GS80, GS160, GS320 [1]
	Tru64 UNIX
	• 4.0F, 4.0G
	  • ASE 1.6
	• 5.0A
	  • TruCluster 5.0A
	• 5.1
	  • TruCluster 5.1
	• 5.1A [1]
	  • TruCluster 5.1A
	• 5.1B [2]
	  • TruCluster 5.1B
		StorageWorks
		• KGPSA-BC
		• KGPSA-CA
		• KGPSA-DA [2]
			IBM
			• 2109 Model F16 [1]
			• 2109 Models S08 and S16
			• 3534 Model F08 [1]

[1] Requires ESS LIC level 1.5.2, or later.

[2] Requires ESS LIC level 2.2.0, or later.

RQS nº 03/2005 - CN
CPMI . CORREIOS
Fls Nº 1224
Doc. 3698

General notes:

- Fibre channel:
  - Requires ESS LIC level 1.3.3.27, or later.
- Copy services:
  - Requires ESS LIC level 1.5.2, or later.
  - Not available for the ESS Models E10 and E20.
- ESS API – CIM Agent:
  - Not Available for Tru64 UNIX.
- ESS CLI:
  - Not available for Tru64 UNIX.
- CS CLI:
  - Available for Tru64UNIX 4.0F, 4.0G, 5.1, 5.1A, and 5.1B.
  - Requires ESS LIC level 1.5.2, or later.
  - Not available for the ESS Models E10 and E20.
- SDD:
  - Not available for Tru64 UNIX.
  - Multi-path support is natively available in Tru64 UNIX.
- Boot device support:
  - The ESS can be used as a boot device on servers running Tru64 UNIX 5.0A and 5.1. This function requires ESS LIC level 1.3.3, or later. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.

- The following items are not interoperable with the ESS Model 800:
  - Operating systems:
    - Tru64 UNIX 4.0 (all levels).

- The following items are not interoperable with the ESS Models E10 and E20:
  - Copy services.
  - CS CLI.
  - Servers:
    - AlphaServers GS80, GS160, and GS320.
  - Operating systems:
    - Tru64 UNIX 5.1A and 5.1B.
  - Fabric products:
    - IBM 3534 Model F08.

10.839

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

9406 Advanced Series
• 300, 310, 320
• 500, 510, 530
 	
9406
• 620, 640, 650
• 720, 730, 740
• S20, S30, S40
 	
iSeries
• 820, 830, 840
• SB2, SB3
	OS/400
	• Version 3
	  • V3R1 @
	  • V3R2 @
	  • V3R6 @
	  • V3R7 @
	• Version 4
	  • V4R1 @
	  • V4R2 @
	  • V4R3 @
	  • V4R4 @
	  • V4R5
	• Version 5
	  • V5R1
	  • V5R2 [1]
		IBM iSeries and AS/400
		• FC 6501
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

iSeries
• 270
• 820, 830, 840, 890 [1]
• 800, 810, 825, and 870 [3]
	OS/400
	• Version 5
	  • V5R1
	  • V5R2 [1]
	
	Linux [2]
	• SuSE Linux Enterprise Server 7 for iSeries
	
	UnitedLinux 1.0 [4]
	• SuSE Linux Enterprise Server 8 (SP 1)
		IBM iSeries
		• FC 0612
		• FC 2766
			IBM
			• 2109 Model F16 [1]
			• 2109 Models S08 and S16
			• 3534 Model 1RU
			• 3534 Model F08 [1]

[1] Requires ESS LIC level 1.5.2, or later.

[2] Requires Linux kernel level 2.4.13, and OS/400 V5R2, or later.

[3] Requires ESS LIC level 1.5.2, or later and OS/400 V5R2, or later.

[4] Requires Linux kernel level 2.4.19, OS/400 V5R2, or later, and ESS LIC level 2.1.1, or later.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1225
Doc. 3698

General notes:

- Fibre channel support:
  - Requires ESS LIC Level 1.3.2, or later.
- Copy services:
  - PPRC-XD requires OS/400 Version 5 Release 1, or later.
- ESS API – CIM Agent:
  - Not Available for OS/400.
- ESS CLI:
  - Not available for OS/400.
- CS CLI:
  - Not available for OS/400.
- SDD:
  - Not available for OS/400.

- The following items are not interoperable with the Model 800:
  - Operating systems:
    - OS/400 Version 3 (all release levels).
    - OS/400 Version 4 (all release levels except V4R5).
  - Fabric products:
    - IBM 3534 Model 1RU.

- The following items are not interoperable with the Models F10 and F20:
  - Operating systems:
    - SuSE Linux Enterprise Server 7 for iSeries.

- The following items are not interoperable with the Models E10 and E20:
  - Servers
    - iSeries 800, 810, 825, 870, and 890.
  - Operating systems:
    - OS/400 Version 5 Release 2.
    - OS/400 Version 4 (all release levels except Release 5).
    - SuSE Linux Enterprise Server 7 for iSeries.
    - UnitedLinux 1.0.
  - Fabric products:
    - IBM 2109 Models F16, S08, and S16.
    - IBM 3534 Model F08.

10.83

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support
2000 • E100 • E200 • E320 • E400, E410 • xSeries 430	ptx (DYNIX) [1] • 4.4.7, 4.4.8, 4.4.9, 4.4.10 • 4.5.1, 4.5.2, 4.5.3 • 4.6.1	IBM NUMA-Q • IOC-0210-54	IBM • 2109 Models S08 and S16

[1] ptx general notes:
- ptx 4.4.7, 4.4.8, 4.4.9, and 4.4.10 interoperability is available only via RPQ (NSBO).
- ptx 4.4.10 requires ESS LIC level 1.4.0, or later.
- ptx 4.5.1 requires service pack 3.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1226
3698
Doc

General Notes:

- NUMA-Q support requires ESS LIC level 1.2.1, or later.
- ESS API – CIM Agent:
  - Not available for ptx.
- ESS CLI:
  - Not available for ptx.
- CS CLI:
  - Available for all levels of ptx.
- SDD:
  - Not available for ptx.

- The following items are not interoperable with the ESS Model 800:
  - Operating systems:
    - ptx 4.4.7, 4.4.8, 4.4.9, and 4.4.10.
    - ptx 4.5.1 and 4.5.2.
    - ptx 4.6.1.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
pSeries • 610 Models 6C1, 6E1 • 615 Models 6C3 and 6E3 • 620 Models 6F0, 6F1 • 630 Models 6C4, 6E4 [1] • 640 Model B80 • 650 Model 6M2 [1] • 655 Model 651 [1] • 660 Models 6H0, 6H1, 6M1 • 670 Model 671 [1] • 680 Model S85 • 690 Model 681 [1] 7012 • 397 • G40 7013 • 590, 591, 595, 59H • J30, J40, J50 • S70, S7A 7015 • 99J, 99K • R20, R24, R30, R40, R50 • S70, S7A 7017 • S70, S7A, S80 7024 • E20, E30 7025 • F30, F40, F50, F80 • H70 7026 • H10, H50, H70, H80 • M80 7043 • 270 7044 • 170 • 270	AIX • Version 4 • 4.2.1 @ • 4.3.1 @ • 4.3.2 @ • 4.3.3 • Version 5 • 5.1 • 5.2 [7] HACMP [2] • 4.2.2 • 4.3.1 • 4.4.0, 4.4.1 • 4.5.0 [3]	IBM pSeries and RS/6000 • FC 2412 • FC 6204 • FC 6207	N/A

[1] ESS LIC level prerequisites for servers:
- The pSeries 630, 650, and 655 require ESS LIC level 1.5.2, or later.
- The pSeries 670 requires ESS LIC level 1.5.1, or later.
- The pSeries 690 requires ESS LIC level 1.4.0, or later.

[2] Refer to Table 4 for additional HACMP support information.

[3] Requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1227
3698
Doc.

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

pSeries
• 610 Models 6C1, 6E1
• 615 Models 6C3 and 6E3
• 620 Models 6F0, 6F1
• 630 Models 6C4, 6E4 [1]
• 640 Model B80
• 650 Model 6M2 [1]
• 655 Model 651 [1]
• 660 Models 6H0, 6H1, 6M1
• 670 Model 671 [1]
• 680 Model S85
• 690 Model 681 [1]
 	
7013
• S70, S7A
 	
7015
• S70, S7A
 	
7017
• S70, S7A, S80
 	
7025
• F50, F80
• H70
 	
7026
• H50, H70, H80
• M80
 	
7043
• 270
 	
7044
• 170
• 270
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2 [7]
	
	HACMP [2]
	• 4.3.1
	• 4.4.0, 4.4.1
	• 4.5.0 [3]
	
	UnitedLinux 1.0 [9]
	• SuSE Linux Enterprise Server 8 (SP 1)
		IBM pSeries and RS/6000
		• FC 6227
		• FC 6228
		• FC 6239 [10]
			Cisco [5]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [4]
			• 2109 Models F16 and F32 [5]
			• 2109 Model M12 [5]
			• 2109 Models S08 and S16
			• 3534 Model F08 [5]
			
			INRANGE
			• FC/9000-64 [6]
			• FC/9000-128 [6]
			• FC/9000- 256 [8]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [5]
			• Sphereon
			  • 3216 [5]
			  • 3232 [5]
			  • 4500 [5]

[4] The IBM 2103 is supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[5] Requires ESS LIC level 1.5.2, or later.

[6] Requires ESS LIC level 1.3.2.50, or later.

[7] Requires ESS LIC level 2.0.1, or later, for the ESS Model 800 and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[8] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[9] Requires Linux kernel level ppc64-2.4.19-186, and ESS LIC level 2.1.1, or later. UnitedLinux 1.0 is supported with only host adapter FC 6228 and only with IBM or McDATA fabric products.

[10] Requires ESS LIC level 2.1.1, or later.

General Notes:

- Fibre channel:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for AIX 5.1.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for AIX 4.3.3, 5.1, and 5.2.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for AIX 4.3.2, 4.3.3, 5.1, and 5.2.
- SDD:
  - Available for AIX 4.3.1, or later.
- Boot device support:
  - The ESS is supported as a boot device on pSeries, RS/6000, and RS/6000 SP servers that support Fibre Channel boot capability. This support requires ESS LIC level 1.4.0, or later, and native Fibre Channel attachment to the ESS. Boot device support when using SDD requires ESS LIC level 2.1.0, or later. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.
- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Servers:
    - Micro Channel Architecture (MCA) servers, including 7012-397, 7013-59x, 7013-Jxx, 7015-99x, and 7015 Rxx.
  - Operating systems:
    - AIX 4.2.1, 4.3.1 and 4.3.2.
    - HACMP 4.2.2 and 4.3.1.
  - Host adapters:
    - IBM FC 2412.
  - Fabric products:
    - IBM 2103 Model H07.
- <u>The following items are not interoperable with the ESS Models E10 and E20</u>
  - ESS API.
  - ESS CLI.
  - SDD
    - Boot Device Support.
  - Operating systems:
    - AIX 5.2.
    - HACMP 4.5.0.
    - UnitedLinux 1.0.
  - Servers:
    - 615 Models 6C3 and 6E3.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

10.833
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1228
Doc 3698

Table 4: AIX and HACMP Support Matrix

	ESS Model 800	ESS Models F10 and F20	ESS Models E10 and E20	SDD
AIX 4.2.1 with HACMP 4.2.2	--	--	SCSI	--
AIX 4.3.3 with HACMP 4.2.2	--	--	SCSI	--
AIX 4.3.3 with HACMP 4.3.1	--	SCSI Fibre Channel	SCSI Fibre Channel	Yes
AIX 4.3.3 with HACMP 4.4.0	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes
AIX 4.3.3 with HACMP 4.4.1	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes [1]
AIX 5.1 with HACMP 4.4.0	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes
AIX 5.1 with HACMP 4.4.1	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes [1]
AIX 5.1 with HACMP 4.5.0	SCSI Fibre Channel	SCSI Fibre Channel	--	Yes
AIX 5.2 with HACMP 4.5.0	SCSI Fibre Channel	SCSI Fibre Channel	--	Yes

[1] RS/6000 SP with SDD and HACMP 4.4.1 requires AIX 5.1 ML2 with ESS LIC level 1.4.0, or later.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

9076 Models 2xx, 3xx, 4xx, 50x, 55x, and T70 with the following nodes:
 	
Micro Channel
• FC 2002: 62MHz Thin Node
• FC 2003: 66MHz Thin Node
• FC 2004: 66MHz Thin Node 2
• FC 2005: 77MHz Wide Node
• FC 2006: 604 High Node
• FC 2007: 35MHz Wide Node
• FC 2008: 120MHz Thin Node
• FC 2009: 604E High Node
• FC 2022: 160MHz Thin Node
 	
PCI
• FC 2050: 332 MHz SMP Single Thin
• FC 2051: 332 MHz SMP Wide Node
• FC 2052: POWER3 SMP Thin Node
• FC 2053: POWER3 SMP Wide Node
• FC 2054: POWER3 SMP High Node
• FC 2055: SP Expansion I/O Unit
• FC 2056: POWER3 375MHz SMP Thin
• FC 2057: POWER3 375MHz SMP Wide
• FC 2058: POWER3 375MHz SMP High
	AIX
	• Version 4
	  • 4.2.1 @
	  • 4.3.1 @
	  • 4.3.2 @
	  • 4.3.3
	• Version 5
	  • 5.1 ML2 [1]
	
	PSSP [2]
	• 3.1, 3.1.1
	• 3.2
		IBM RS/6000
		• FC 2412
		• FC 6204
		• FC 6207
		• FC 6209
			N/A

[1] Requires ESS LIC level 1.4.0, or later.

[2] Refer to Table 5 for additional PSSP information. Refer to Table 4 (pSeries and RS/6000 server section) for HACMP information.

10.831
J
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1229
Doc 3698

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

9076 Models 2xx, 3xx, 4xx, 50x, 55x, and T70 with the following PCI nodes:
• FC 2050: 332 MHz SMP Single Thin Node
• FC 2051: 332 MHz SMP Wide Node
• FC 2052: POWER3 SMP Thin Node
• FC 2053: POWER3 SMP Wide Node
• FC 2054: POWER3 SMP High Node
• FC 2055: SP Expansion I/O Unit
• FC 2056: POWER3 375MHz SMP Thin Node
• FC 2057: POWER3 375MHz SMP Wide Node
• FC 2058: POWER3 375MHz SMP High Node
	AIX
	• Version 4
	  • 4.3.3
	• Version 4
	  • 5.1 ML2 [1]
	
	PSSP [2]
	• 3.1.1
	• 3.2
	• 3.4
		IBM RS/6000
		• FC 6227
		• FC 6228
			Cisco [4]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [3]
			• 2109 Models F16 and F32 [4]
			• 2109 Model M12 [4]
			• 2109 Models S08 and S16
			• 3534 Model F08 [4]
			
			INRANGE
			• FC/9000-64 [5]
			• FC/9000-128 [5]
			• FC/9000- 256 [6]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [4]
			• Sphereon
			  • 3216 [4]
			  • 3232 [4]
			  • 4500 [4]

[3] The IBM 2103 is supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1.5.2, or later.

[5] Requires ESS LIC level 1.3.2.50, or later.

[6] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

10.329

General Notes:

- Fibre channel:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for AIX 5.1 ML2.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for AIX 4.3.3 and 5.1.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for AIX 4.3.2, 4.3.3, and 5.1.
- SDD:
  - Available for AIX 4.3.3, or later
  - Requires ESS LIC level 1.3.2.50, or later.
  - Refer to Table 5 for additional information.
- Boot device support:
  - The ESS is supported as a boot device on pSeries, RS/6000, and RS/6000 SP servers that support Fibre Channel boot capability. This support requires ESS LIC level 1.4.0, or later, and native Fibre Channel attachment to the ESS. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.
- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Servers:
    - Micro Channel Architecture (MCA) servers, including 7012-397, 7013-59x, 7013-Jx, 7015-99x, and 7015 Rxx.
  - Operating systems:
    - AIX 4.2.1, 4.3.1 and 4.3.2.
    - HACMP 4.2.2 and 4.3.1.
  - Host adapters:
    - IBM FC 2412.
  - Fabric products:
    - IBM 2103 Model H07.
- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - ESS API.
  - ESS CLI.
  - Operating systems:
    - HACMP 4.5.0
  - Fabric products:
    - Cisco MDS 9216, and 9509.
    - IBM 2109 Model F32.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 4500

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1230
Doc 3698

Table 5: AIX, PSSP, and SDD Support Matrix

	ESS Model 800	ESS Models F10 and F20	ESS Models E10 and E20	SDD Level
AIX 4.3.2 with: • PSSP and RVSD 3.1.0 • GPFS 1.2	--	SCSI	SCSI	--
AIX 4.3.3 with: • PSSP and RVSD 3.1.1 • GPFS 1.2	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	1.2.1.3
AIX 4.3.3 with: • PSSP and RVSD 3.2 • GPFS 1.3 or 1.4	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	1.2.1.3
AIX 5.1 with: • PSSP 3.4 • GPFS 1.5	Fibre Channel	Fibre Channel	Fibre Channel	1.3.1.1

ESCON

Servers	Operating Systems	Host Adapters	Fabric Support
zSeries z800 • IBM 2066 zSeries z900 and z990 • IBM 2064 S/390 Parallel Enterprise Server • IBM 9672 Generation 3 • IBM 9672 Generation 4 • IBM 9672 Generation 5 • IBM 9672 Generation 6 ES/9000 • IBM 9021 • IBM 9121 • IBM 9221 ES/3090 • IBM 3090 S/390 Multiprise 3000 Enterprise Server • IBM 7060 S/390 Multiprise 2000 Enterprise Server • IBM 2003	z/OS • Version 1 Release 1 • Version 1 Release 2 • Version 1 Release 3 • Version1 Release 4 [1] z/OS.e • Version 1 Release 3 • Version 1 Release 4 [1] OS/390 • Version 1 Release 3 @ • Version 2 Release 4 @ • Version 2 Release 5 @ • Version 2 Release 6 @ • Version 2 Release 7 @ • Version 2 Release 8 @ • Version 2 Release 9 @ • Version 2 Release 10 z/VM • Version 3 Release 1 @ • Version 4 Release 1 @ • Version 4 Release 2 • Version 4 Release 3 • Version 4 Release 4 [5] VM/ESA • Version 2 Release 2 @ • Version 2 Release 3 @ • Version 2 Release 4 @ VSE/ESA • Version 2 Release 1 @ • Version 2 Release 2 @ • Version 2 Release 3 @ • Version 2 Release 4 @ • Version 2 Release 5 • Version 2 Release 6 • Version 2 Release 7 Transaction Processing Facility (TPF) [2] • Version 4 Release 1 Linux for S/390 • SuSE Linux Enterprise Server for S/390 • Turbolinux Server 6 for zSeries and S/390 • SuSE SLES 8 for zSeries and S/390 [3]	All ESCON host adapter features offered on the servers are supported.	IBM • 9032 Model 002 • 9032 Model 003 • 9032 Model 005

[1] Requires ESS LIC level 1.5.2, or later.

[2] In the TPF environment, PPRC and FlashCopy require ESS LIC level 1.5.0, or later.

[3] Requires ESS LIC Level 2.1.1 or later, direct connect only.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1231
Doc. 3698

FICON

Servers	Operating Systems	Host Adapters	Fabric Support
zSeries z800 • IBM 2066 zSeries z900 and z990 • IBM 2064 S/390 Parallel Enterprise Server • IBM 9672 Generation 5 • IBM 9672 Generation 6	z/OS • Version 1 Release 1 • Version 1 Release 2 • Version 1 Release 3 • Version 1 Release 4 [1] z/OS.e • Version 1 Release 3 • Version 1 Release 4 [1] OS/390 • Version 2 Release 8 @ • Version 2 Release 9 @ • Version 2 Release 10 z/VM • Version 3 Release 1 @ • Version 4 Release 1 @ • Version 4 Release 2 • Version 4 Release 3 • Version 4 Release 4 [5] VM/ESA • Version 2 Release 3 @ • Version 2 Release 4 @ VSE/ESA • Version 2 Release 3 @ • Version 2 Release 4 @ • Version 2 Release 5 • Version 2 Release 6 • Version 2 Release 7 Transaction Processing Facility (TPF) [2] • Version 4 Release 1 Linux for zSeries and S/390 [3] • SuSE SLES 8	zSeries • FC 2315 • FC 2318 • FC 2319 • FC 2320 S/390 • FC 2314 • FC 2316	INRANGE • FC/9000-64 • FC/9000-128 • FC/9000-256 [4] McDATA • ED-5000 • Intrepid 6064 • Intrepid 6140 [1]

[4] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[5] Requires ESS LIC level 2.2.0, or later.

10.825

Fibre Channel Protocol (FCP)

Servers	Operating Systems	Host Adapters	Fabric Support
zSeries z800 • IBM 2066 zSeries z900 and z990 • IBM 2064	UnitedLinux 1.0 • SuSE SLES 8 (SP 2)	zSeries • FC 2315 • FC 2318 • FC 2319 • FC 2320	IBM • 2109 Model F16 • 2109 Models S08 and S16 INRANGE • FC/9000-64 • FC/9000-128 McDATA • Intrepid 6064

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1232
Doc. 3698

General Notes:

- ESCON:
  - IBM eServer Integrated Platform for e-business on zSeries, and S/390 G5 and G6:
    - Supported on ESS Models F20 and F10, and requires ESS LIC level 2.1.1, or later.
    - Requires zVM Version 4 Release 3.
    - Requires Linux SLES 7, with kernel level 2.4.7.
- FICON:
  - Requires ESS LIC level 1.4.0, or later.
  - FICON is not supported on the ESS Models E10 and E20.
- Fibre Channel Protocol (FCP):
  - Requires ESS LIC level 2.1.1, or later.
  - FCP is not supported on the ESS Models E10 and E20.
  - Multipath support is available with LVM.
- Copy Services
  - Supported in the Linux for zSeries and S/390 environment with SuSE SLES 8.
- ESS API – CIM Agent:
  - Not available for zSeries and S/390 operating systems.
- ESS CLI:
  - Not available for zSeries and S/390 operating systems.
- CS CLI:
  - Not available for zSeries and S/390 operating systems.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Operating systems:
    - OS/390 levels 1.3, 2.4, 2.5, 2.6, 2.7, 2.8, and 2.9.
    - VM/ESA levels 2.2 and 2.3.
    - VSE/ESA levels 2.1, 2.2, and 2.3.
    - IBM eServer Integrated Platform for e-business on zSeries.

- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - FCP.
  - FICON.
  - Operating systems:
    - z/OS level 1.4.
    - z/OS.e level 1.4.
    - z/VM level 4.4.
    - VSE/ESA level 2.7.
    - IBM eServer Integrated Platform for e-business on zSeries.
  - Fabric products:
    - McDATA Intrepid 6140.
  - ESS copy services in the TPF environment.

This page is intentionally left blank.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1233
Doc. 3698

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later processors
• 200 MHz processor or faster
• 128 MB memory or greater
• Excludes IBM Netfinity 3000 and IBM PC Server 325
 	
IBM eServer BladeCenter [8]
• BladeCenter HS20
	Red Hat Linux
	• 7.1 [1]
	• 7.2 [1]
	• 7.3 [1]
	
	Red Hat Enterprise Linux Advanced Server
	• 2.1 [2]
	
	SuSE Linux
	• 7.2
	• 7.3
	
	SuSE Linux Enterprise Server (SLES)
	• 7 [3]
	
	UnitedLinux 1.0 [7]
	• SuSE Linux Enterprise Server 8 (SP 1 and SP 2a)
		Emulex
		• LP9002L / LP9002DC [4]
		• LP9402DC [4]
		• LP9802 [4]
		
		IBM BladeCenter
		• P/N 48P7062
		
		QLogic
		• QLA2300F
		• QLA2310F / QLA2310FL [4]
		• QLA2340/L / QLA2342/L [5]
			Cisco [4]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2109 Models F16 and F32 [4]
			• 2109 Model M12 [4]
			• 2109 Models S08 and S16
			• 3534 Model F08 [4]
			
			INRANGE
			• FC/9000-64
			• FC/9000-128
			• FC/9000- 256 [6]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [4]
			• Sphereon
			  • 3216 [4]
			  • 3232 [4]
			  • 4500 [4]

[1] Red Hat 7.x requires kernel level 2.4.18-24.7xbigmen, and ESS LIC level 2.1.1, or later.

[2] Red Hat Enterprise Advanced Server 2.1 requires kernel level 2.4.9-e.16 (enterprise or summit for x440 server), or kernel level 2.4.9-e.24 QU2 (enterprise), and ESS LIC 2.1.1, or later.

[3] SuSE Linux Enterprise Server 7 Update requires kernel level k_smp-2.4.18-224, and ESS LIC level 2.1.1, or later.

[4] Requires ESS LIC level 1.5.2, or later.

[5] Requires ESS LIC level 2.1.0, or later.

[6] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[7] Requires SP 1 kernel level k_smp-2.4.19-233, SP 2a kernel level k_smp-2.4.19-304, and ESS LIC level 2.2.0, or later.

[8] Requires ESS LIC level 2.1.1, or later, and Red Hat Linux Advanced Server 2.1, kernel level 2.4.9.e.16. The following fabric products are supported: IBM 2109 Model F16, IBM 3534 Model F08, INRANGE, and McDATA (excluding ED-5000).

General Notes:

- Linux is interoperable with only the ESS Models F10, F20, and 800.
- ESS API – CIM Agent:
  - Available for Red Hat Linux 7.2.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for Red Hat 7.2, and 7.3.
  - Available for UnitedLinux 1.0 (SLES 8).
  - Requires ESS LIC level 2.1.0, or later.
- CS CLI:
  - Available for all levels of Linux.
- SDD:
  - Available for Red Hat 7.2 and Red Hat Enterprise Advanced Server 2.1.
  - Available for SuSE 7.3 and SuSE Linux Enterprise Server 7.
  - Available for UnitedLinux 1.0 (SLES 8).
  - SDD is not interoperable with BladeCenter.
- The following SuSE and Redhat levels are no longer recommended with the ESS. If problems are encountered with existing installations, you may be required to update your Linux configuration to a higher level before problem determination can take place.
  - Red Hat Linux 7.1 running kernel level 2.4.9.
  - Red Hat Linux 7.2 running kernel level 2.4.9-31.
  - Red Hat Linux Advanced Server 2.1 running kernel levels 2.4.9-e.8 and 2.4.9-e.10 (enterprise).
  - SuSE Linux 7.2 running kernel level 2.4.9.
  - SuSE Linux 7.3 running kernel level k_smp-2.4.16-22.
  - SuSE Linux Enterprise Server (SLES) 7 running kernel level 2.4.18-134.
- <u>The following items are not interoperable with the Model 800:</u>
  - Operating systems:
    - Red Hat Linux 7.1.
    - SuSE Linux 7.2.
- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - BladeCenter.
  - ESS API
  - Host Adapters:
    - Emulex LP9402DC and LP9802.
  - Fabric products
    - Cisco MDS 9216 and MDS 9509
    - INRANGE FC/9000- 256
  - Operating Systems:
    - UnitedLinux 1.0.

10.822

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1234
3698
Doc.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later processors
• 200 MHz processor or faster
• 128 MB memory or greater
	Novell NetWare
	• 4.11 @
	• 4.2
	  • Standby Server
	• 5.0
	  • Cluster Services 1.00
	  • Cluster Services 1.01
	• 5.1
	  • Cluster Services 1.01
	• 6.0 [1]
		Adaptec
		• AHA-2944UW
		
		IBM xSeries / Netfinity
		• P/N 08L6517 [2]
		• P/N 59H3900
		
		QLogic
		• QLA1041
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later processors
• 200 MHz processor or faster
• 128 MB memory or greater
• Excludes IBM Netfinity 3000 and IBM PC Server 325
	Novell NetWare
	• 4.2
	  • Standby Server
	• 5.0
	  • Cluster Services 1.00
	  • Cluster Services 1.01
	• 5.1
	  • Cluster Services 1.01
	• 6.0 [1]
	  • Cluster Services 1.6
		Emulex
		• LP9002L / LP9002DC [1]
		• LP9402DC [1]
		• LP9802 [1]
		
		IBM xSeries / Netfinity
		• P/N 01K7297
		• P/N 00N6881
		• P/N 19K1246
		• P/N 24P0960
		
		QLogic
		• QLA2100F
		• QLA2200F
		• QLA2310F / QLA2310FL [1]
		• QLA2340/L / QLA2342/L [1]
			Cisco [1]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [3]
			• 2109 Models F16 and F32 [1]
			• 2109 Model M12 [1]
			• 2109 Models S08 and S16
			• 3534 Model 1RU [3]
			• 3534 Model F08 [1]
			
			INRANGE
			• FC/9000-64 [4]
			• FC/9000-128 [4]
			• FC/9000- 256 [5]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064 [4]
			  • 6140 [4]
			• Sphereon
			  • 3216 [4]
			  • 3232 [4]
			  • 4500 [1]

[1] Requires ESS LIC level 1.5.2, or later.
- Planned availability is 4Q03 for the Emulex LP9402DC and LP9802 host adapter interoperability.

[2] Host adapter IBM P/N 08L6517 includes an incorrect SCSI cable for ESS attachment. Order ESS feature number 9701 / 2801 (10 meter) or feature number 9702 / 2802 (20 meter) to obtain the correct SCSI cable to use this host adapter with the ESS.

[3] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1.5.2, or later, and NetWare 5.1 or later.

[5] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

General Notes:

- Fibre Channel support:
  - Requires ESS LIC level 1.3.0, or later.
- Clustering support:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Not available for NetWare.
- ESS CLI:
  - Not available for NetWare.
- CS CLI:
  - Available for NetWare 4.2 and NetWare 5.1, or later.
  - NetWare 6.0 requires ESS LIC 2.1.0, or later.
- SDD:
  - Refer to the *IBM TotalStorage Enterprise Storage Server Subsystem Device Driver User's Guide* for support information when running NetWare 5.1 and 6.0 with SDD.
  - Requires NetWare 5.1, or later, and ESS LIC level 2.1.0, or later.
  - Not interoperable with the Emulex LP9002L / LP9002DC, LP9402DC, and LP9802.
  - Not available for the ESS Model E10 and E20.
  - NetWare 6.0 cluster services supported on fibre channel only.

- The following items are not interoperable with the ESS Model 800:
  - Operating systems:
    - NetWare 4.11 and 4.2.
  - Host adapters:
    - IBM P/N 01K7297.
    - QLogic QLA1041 and QLA2100F.
  - Fabric products:
    - IBM 2103 Model H07.
    - IBM 3534 Model 1RU.

- The following items are not interoperable with the ESS Models E10 and E20:
  - CS CLI:
    - NetWare 6.0.
  - SDD.
  - Operating systems:
    - NetWare 6.0.
  - Host adapters:
    - Emulex LP90002L.
    - Emulex LP9002L / LP9002DC.
    - Emulex LP9402DC and LP9802.
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
  - Fabric products:
    - IBM 2109 Models F32, and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1235
Doc. 3698

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
Pentium Pro or later 32 bit processors • 200 MHz processor or faster • 128 MB memory or greater	Microsoft Windows NT • Server 4.0 • Server 4.0, Enterprise Edition including Microsoft Cluster Server (MSCS) Microsoft Windows 2000 • Server • Advanced Server including Cluster service Microsoft Windows Server 2003 [6] • Standard Edition • Enterprise Edition including cluster service	Adaptec • AHA-2944UW IBM Netfinity/xSeries • P/N 08L6517 [1] • P/N 59H3900 QLogic • QLA1041 Symbios • LSI8751D	N/A

[1] Host adapter IBM 08L6517 includes an incorrect SCSI cable for ESS attachment. Order ESS feature number 9701 / 2801 (10 meter) or feature number 9702 / 2802 (20 meter) to obtain the correct SCSI cable to use this host adapter with the ESS.

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later 32 bit processors
• 200 MHz processor or faster
• 128 MB memory or greater
• Excludes IBM Netfinity 3000 and IBM PC Server 325
 	
IBM eServer BladeCenter [7]
• BladeCenter HS20
	Microsoft Windows NT
	• Server 4.0
	• Server 4.0, Enterprise Edition including Microsoft Cluster Server (MSCS)
	
	Microsoft Windows 2000
	• Server
	• Advanced Server including Cluster service
	• Datacenter Server
	
	Microsoft Windows Server 2003 [6]
	• Standard Edition
	• Enterprise Edition including cluster service
	• Datacenter Edition including cluster server
		Emulex
		• LP7000E
		• LP8000
		• LP9002L / LP9002DC [2]
		• LP9402DC [2]
		• LP9802 [2]
		
		IBM BladeCenter
		• P/N 48P7062
		
		IBM Netfinity/xSeries
		• P/N 01K7297
		• P/N 00N6881
		• P/N 19K1246
		• P/N 24P0960
		
		QLogic
		• QLA2100F
		• QLA2200F
		• QLA2310F / QLA2310FL [2]
		• QLA2340/L / QLA2342/L [2]
			Cisco [2]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [3]
			• 2109 Models F16 and F32 [2]
			• 2109 Model M12 [2]
			• 2109 Models S08 and S16
			• 3534 Model F08 [2]
			• 3534 Model 1RU [3]
			
			INRANGE
			• FC/9000-64 [4]
			• FC/9000-128 [4]
			• FC/9000- 256 [5]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064 [2]
			  • 6140 [2]
			• Sphereon
			  • 3216 [2]
			  • 3232 [2]
			  • 4500 [2]

[2] Requires ESS LIC level 1.5.2, or later.

[3] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1.3.2.50, or later.

[5] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[6] Requires ESS LIC level 2.2.0, or later. Windows 2003 is not supported on the Emulex LP7000E, QLogic QLA2100F, and IBM P/N 01K7297 host adapters, and the Cisco fabric switches.

[7] Requires ESS LIC level 2.1.1, or later, and is supported on only Windows 2000 (non-clustered configurations). The following fabric products are supported: IBM 2109 Model F16, IBM 3534 Model F08, INRANGE, and McDATA (excluding ED-5000).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1236
3698
Doc.

General Notes:

- Fibre channel support:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for all levels of Windows 2000.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for all levels of Windows 2000, and Windows Server 2003.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for all levels of Windows NT, Windows 2000, and Windows Server 2003.
- SDD:
  - Available for all levels of Windows NT and Windows 2000 and Windows 2003 (see additional notes on following page)
  - Load balancing is not available in Windows NT or Windows 2000 cluster configurations.
- Boot device support:
  - The ESS is supported as a boot device on Windows 2000 servers that support Fibre Channel boot capability. This support requires ESS LIC level 2.2.0, or later, with host adapters QLA2310F / QLA2310FL, and QLA2340 / QLA2342L. Requires SDD level 1.4.0.0. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Host adapters:
    - Emulex LP7000E.
    - IBM 01K7297.
    - QLogic QLA1041 and QLA2100F.
    - Symbios SYM8751D.
  - Fabric products:
    - IBM 2103 Model H07.
    - IBM 3534 Model 1RU.

- <u>The following items are not interoperable with the ESS Models E10 and E20</u>
  - BladeCenter.
  - ESS CLI.
  - Operating systems:
    - Datacenter Server.
  - Host adapters:
    - Emulex LP9002L / LP9002DC.
    - ~~Emulex LP9802 and LP9402DC.~~
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
  - ESS API.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - ~~McDATA Sphereon 3216, 3232, and 4500.~~

90.816
J

General Notes (cont.):

- **Windows NT**
  - Enterprise Edition with Microsoft Cluster Server (MSCS) support requires ESS LIC level 1.3.0, or later.
- **Windows 2000**
  - Server and Advanced Server:
    - Requires ESS LIC Level 1.2.0, or later.
    - Advanced Server with Cluster service support requires ESS LIC level 1.3.0, or later.
    - When using SDD, Advanced Server with Cluster service support requires ESS LIC level 1.4.0, or later. The QLogic QLA2100F is not supported in this configuration.
  - Datacenter Server:
    - Requires ESS LIC level 1.5.0, or later.
    - When using SDD, Datacenter Server requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.
    - For a list of specific ESS configurations supported with Datacenter Server, refer to the Microsoft Hardware Compatibility Listing (HCL) at http://www.microsoft.com/hcl/. Enter "Enterprise Storage Server" and "All Product Categories" as the search criterion. Use the IBM RPQ process to request support for additional ESS configurations.
- **Windows 2003**
  - When using clustering with SDD, Windows 2003 is not supported on Emulex LP8000, LP9002L / LP9002DC, LP9402DC, LP9802 host adapters.

ROS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1237
3698
Doc.

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support
Origin Servers • 200 • 2100 • 2200 • 2400 • 2800	IRIX • 6.5.13 • 6.5.14 • 6.5.15 • 6.5.16 • 6.5.17	SGI • PCI-FC-1P-OPT • PCI-FC-1P-OPT-A • PCI-FC-1POPT-B [3] • PCX-FC-2POPT-B [3]	IBM[1] • 2109 Models S08 and S16 • 2109 Model F16 • 3534 Model F08

[1] Cascaded switches are not supported.

[3] Requires ESS LIC level 2.2.0, or later.

General Notes:

- SGI support requires ESS LIC level 2.1.1, or later.
- ESS API – CIM Agent:
  - Not available for IRIX.
- ESS CLI:
  - Not available for IRIX.
- CS CLI:
  - Not available for IRIX.
- SDD:
  - Not available for IRIX.

- The following items are not interoperable with the ESS Models E10 and E20:
  - SGI Servers
    - Origin 200, 2100, 2200, 2400, and 2800

10.844
3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1238
Doc. 3698

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

Enterprise
• 220R, 250, 420R, 450
• 3000, 4000, 5000, 6000
• 3500, 4500, 5500, 6500
• 10000
 	
Netra
• 1125
 	
SPARCcenter / SPARCserver
• 1000, 1000E
• 2000, 2000E
 	
Ultra
• 1, 2, 5, 10, 20, 30, 60, 80
	Solaris
	• 2.5.1
	• 2.6
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2 and 1.3
	• 7
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2 and 1.3
	• 8
	  • VERITAS Volume Manager with DMP
	  • 3.1.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.3
		Sun
		• X1062A
		• X1065A
		• X6541A
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Enterprise
• 220R, 250, 420R, 450
• 3000, 4000, 5000, 6000
• 3500, 4500, 5500, 6500
• 10000
 	
Netra
• 1125
 	
SPARCcenter / SPARCserver
• 1000, 1000E
• 2000, 2000E
 	
Sun Fire
• V120 [1]
• V280R [1]
• V480 [1]
• V880 [1]
• 3800 [1]
• 4800 [1], 4810 [1], 6800 [1]
• 12K [2], 15K [2]
 	
Ultra
• 1,2, 5, 10, 20, 30, 60, 80
	Solaris
	• 2.6
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2, 1.3, 2.0, and 3.5 [3]
	• 7
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2, 1.3 2.0, and 3.5 [3]
	• 8
	  • Sun Cluster 3.0 with MPxIO 4.1, or later [10]
	  • VERITAS Volume Manager with DMP
	  • 3.1.1, 3.2, and 3.5
	  • VERITAS Cluster Server
	  • 1.3, 2.0, and 3.5 [3]
	• 9 [3,7]
	  • VERITAS Volume Manager with DMP
	  • 3.5
	  • VERITAS Cluster Server
	  • 3.5
		JNI
		• FC64-1063-N
		• FCC-6562 / FCC2-6562 [3]
		• FCX-6562 / FCX2-6562 [3]
		• FCI-1063-N
		• FCE-1473-N [1]
		• FCE-6460-N [1]
		
		Emulex
		• LP8000
		• LP8000S [4]
		• LP9002C [3]
		• LP9002L / LP9002DC [1]
		• LP9002S [1]
		• LP9402DC [1]
		• LP9802 [1]
		
		QLogic
		• QLA2200F
		• QLA2310F / QLA2310FL [1]
		• QLA2340/L / QLA2342/L [1]
		• QCP2340 [9]
		
		Sun [10]
		• 6727A
		• 6767A
		• 6768A
		• 6799A
			Cisco [1]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [5]
			• 2109 Models F16 and F32 [1]
			• 2109 Model M12 [1]
			• 2109 Models S08 and S16
			• 3534 Model F08 [1]
			
			INRANGE
			• FC/9000-64 [6]
			• FC/9000-128 [6]
			• FC/9000- 256 [8]
			
			McDATA
			• ED 5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [1]
			• Sphereon
			  • 3216 [1]
			  • 3232 [1]
			  • 4500 [1]

[1] Requires ESS LIC level 1.5.2, or later.

[2] Requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.

[3] Requires ESS LIC level 2.1.0, or later.

[4] Requires ESS LIC level 1.5.0, or later.

[5] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[6] Requires ESS LIC level 1.3.2.50, or later.

[7] Requires Veritas Filesystem VXFS V 3.5 REV=GA06

[8] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[9] Requires 2.1.1, or later.

[10] Requires ESS LIC level 2.2.0, or later. Sun Clustering 3.0 with MPxIO is supported only with the Sun host adapters.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1239
Doc. 3698

General Notes:

- Fibre channel support:
  - Requires ESS LIC level 1.3.0, or later.
- ESS API – CIM Agent:
  - Not Available for Solaris.
- ESS CLI:
  - Available for Solaris 8.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for only Solaris 2.6, 7, 8, and 9.
- SDD:
  - Available for only Solaris 2.6, 7, and 8. (SDD is not supported in Sun Cluster environments.)
  - Solaris 7, or later is required when using the Emulex LP8000.
  - In clustered configurations, VERITAS Cluster Manager and VERITAS Volume Manager with DMP should be used instead of SDD.
  - SDD is not supported in Sun Cluster environments.
- VERITAS:
  - Support for VERITAS Volume Manager is limited to Solaris 7 when using ESS LIC level 1.0.x, 1.1.x or 1.2.x.

- The following items are not interoperable with the ESS Model 800:
  - Operating systems:
    - Solaris 2.5.1.
  - Fabric products:
    - IBM 2103 Model H07.
- The following items are not interoperable with the ESS Models E10 and E20
  - ESS CLI.
  - Servers:
    - Sunfire V120, V280R, V480, V880, 3800, 4800, 4810, 6800, 12K, and 15K.
  - Host adapters:
    - JNI FCC2-6562, FCS-6562 / FCX2-6562, FCE-1473-N and FCE6460-N.
    - Emulex LP9002C, LP9002L / LP9002DC, LP9002S, and LP9402DC, and LP9802.
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
    - Sun 6727A, 6767A, 6768A, and 6799A.
  - Operating Systems:
    - Sun cluster 3.0 and MPxIO.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32, and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

NETWORK ATTACHED STORAGE (NAS)

NAS Servers[1]	Fabric Support
NAS Gateway 300 • 5196 Model G00 • 5196 Model G01 • 5196 Model G02 [3] • 5196 Model G25 • 5196 Model G26 • 5196 Model G27 [2]	IBM • 2109 Models S08 and S16 • 2109 Models F16, and F32 [3] INRANGE • FC/9000 McDATA • ED-5000

[1] NAS interoperability requires ESS LIC level 1.3.2.49, or later.

[2] Requires ESS LIC level 2.0.1, or later, for the ESS Model 800 and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[3] Requires ESS LIC level 1.5.2 or later.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1240
Doc. 3698

General Notes:

- The following items are not interoperable with the ESS Models E10 and E20
  - NAS Gateway 300
    - 5196 Model G00
    - 5196 Model G01
    - 5196 Model G02
    - 5196 Model G25
    - 5196 Model G26
    - 5196 Model G27

APPENDIX A: ESS HOST ADAPTERS AND CABLES

Table 6: ESS Host Adapter Features

Feature Number	Features Description	Supported ESS Models	Minimum ESS LIC Level
3002	SCSI Host Adapter	Exx / Fxx / 800	1.0.0
3011	Standard ESCON Host Adapter	Exx / Fxx	1.0.0
3012	Enhanced ESCON Host Adapter	Fxx / 800	1.4.0
3013	64-bit ESCON Host Adapter	800	2.1.0
3019 [1]	Fibre Channel Host Adapter (interim NUMA-Q)	Exx / Fxx	1.1.0
3020 [1]	Fibre Channel Host Adapter (interim)	Exx / Fxx	1.1.0
3021	Fibre Channel / FICON Host Adapter (long wave)	Fxx	1.4.0
3022	Fibre Channel Host Adapter (short wave)	Exx / Fxx	1.2.0
3023	Fibre Channel / FICON Host Adapter (short wave)	Fxx	1.4.0
3024	2Gb Fibre Channel / FICON Host Adapter (long wave)	800	2.0.0
3025	2Gb Fibre Channel / FICON Host Adapter (short wave)	800	2.0.0

Table 7: ESS Fibre Channel / FICON Cable Features

Specify Feature	Optional Feature	Feature Description	Cable Length
9750	2850	9 micron Fibre Cable (SC connectors)	31 meters
9751	2851	9 micron Fibre Cable (SC / LC connectors)	31 meters
9752	2852	9 micron Fibre Cable (LC connectors)	31 meters
9753	2853	9 micron Fibre Cable (SC / LC connectors)	2 meters (pigtail)
9760	2860	50 micron Fibre Cable (SC connectors)	31 meters
9761	2861	50 micron Fibre Cable (SC / LC connectors)	31 meters
9762	2862	50 micron Fibre Cable (LC connectors)	31 meters
9763	2863	50 micron Fibre Cable (SC / LC connectors)	2 meters (pigtail)

Table 8: ESS SCSI Cable Features

Specify Feature	Optional Feature	Feature Description	Cable Length
9701	2801	Ultra SCSI	10 meters
9702	2802	Ultra SCSI	20 meters
9703	2803	SCSI-2 Fast/Wide	10 meters
9704	2804	SCSI-2 Fast/Wide	20 meters
9705	2805	SCSI-2 Fast/Wide (AS/400)	10 meters
9706	2806	SCSI-2 Fast/Wide (AS/400)	20 meters
9707	2807	SCSI-2 Fast/Wide (Sun PCI/HP PCI dual port)	10 meters
9708	2808	SCSI-2 Fast/Wide (Sun PCI/HP PCI dual port)	20 meters
9709	2809	SCSI-2 Fast/Wide (HP single port)	10 meters
9710	2810	SCSI-2 Fast/Wide (HP single port)	20 meters

[1] Withdrawn from marketing.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls. Nº 1241
3698
Doc.

APPENDIX B: HOST ADAPTER PRODUCTS

Table 9: SCSI Host Adapters

Adapter	Description	ESS Cable Feature
Adaptec AHA-2944UW	PCI-to-Ultra Wide Differential SCSI Host Adapter	9701 or 9702
Adaptec AHA-4944W	Quad Channel PCI-to-Fast and Wide Differential SCSI Host Adapter	9701 or 9702
Hewlett-Packard A4800A	Fast/Wide Ultra Differential SCSI-2 (PCI)	9709 or 9710
Hewlett-Packard A4107A	Fast/Wide Differential SCSI-2 (HP-HSC)	9703 or 9704
Hewlett-Packard A2969A	20 MB Fast/Wide Differential SCSI-2 (HP-HSC)	9703 or 9704
Hewlett-Packard A5159A	Dual Port Fast/Wide Differential SCSI-2 (PCI)	9707 or 9708
Hewlett-Packard 28696A	Fast/Wide Differential SCSI-2 (HP-PB)	9703 or 9704
IBM AS/400 FC 6501	Tape/Disk Device Controller	9705 or 9706
IBM Netfinity P/N 59H3900	3449 Adapter Card	9701 or 9702
IBM Netfinity P/N 08L6517	Adapter card + cable + terminator	9701 or 9702
IBM RS/6000 FC 2412	Enhanced SCSI-2 Differential Fast/Wide Adapter/A	9703 or 9704
IBM RS/6000 FC 6204	PCI Universal Differential Ultra SCSI Adapter	9701 or 9702
IBM RS/6000 FC 6207	PCI Differential Ultra SCSI Adapter	9701 or 9702
IBM RS/6000 FC 6209	PCI SCSI-2 Fast/Wide Differential Adapter	9703 or 9704
QLogic QLA1041	PCI-to-Ultra SCSI Host Adapter	9701 or 9702
Storage Works KZPBA-CB	Ultra SCSI Differential Adapter (PCI)	9701 or 9702
Sun X1062A	SCSI-2 Fast/Wide Differential (SBus)	9701 or 9702
Sun X1065A	Ultra SCSI (SBus)	9701 or 9702
Sun X6541A	Ultra SCSI-2, Fast/Wide Differential Dual Channel (PCI)	9707 or 9708
Symbios SYM8751D	PCI-to-Fast/Ultra Wide Differential SCSI Host Adapter	9701 or 9702

Table 10: Fibre Channel Host Adapters

Adapter	Description
Emulex LP7000E	LightPulse Fibre Channel PCI Host Adapter (32 bit)
Emulex LP8000	LightPulse Fibre Channel PCI Host Adapter (1Gb)
Emulex LP8000S	LightPulse Fibre Channel SBus Host Adapter (1Gb)
Emulex LP9000C	LightPulse Fibre Channel cPCI Host Bus Adapters (2Gb)
Emulex LP9002L	LightPulse Fibre Channel PCI Host Adapter (2Gb)
Emulex LP9002DC	Light Pulse Fibre Channel PCI Host Adapter (2Gb) (two ports)
Emulex LP9002S	LightPulse Fibre Channel SBus Host Adapter (2Gb)
Emulex LP9402DC	LightPulse Fibre Channel PCI-X Host Adapter (2Gb) (two ports)
Emulex LP9802	LightPulse Fibre Channel PCI-X Host Adapter (2GB)
Hewlett-Packard A3404A	1063 Mbps Fibre Channel K Class Adapter (HP-HSC)
Hewlett-Packard A3591B	1062 Mbps Fibre Channel Adapter (HP-HSC)
Hewlett-Packard A5158A	PCI Tachlite Fibre Channel Adapter
Hewlett-Packard A6684A	HSC Tachlite Fibre Channel Adapter
Hewlett-Packard A6685A	HSC Tachlite Fibre Channel Adapter
Hewlett-Packard A6795A	PCI Tachlite 2Gb Fibre Channel Adapter
IBM iSeries FC0612	Linux Direct Attachment
IBM iSeries FC 2766	PCI Fibre Channel Disk Controller
IBM Netfinity P/N 01K7297	Netfinity PCI Fibre Channel Adapter
IBM Netfinity P/N 00N6881	Netfinity FAStT Host Adapter
IBM NUMA-Q IOC-0210-54	Fibre Channel PCI Adapter
IBM pSeries FC 6227	Fibre Channel Adapter for PCI Bus
IBM pSeries FC 6228	Fibre Channel Adapter 64-Bit for PCI Bus (2Gb)
IBM pSeries FC 6239	Fibre Channel Adapter 64-bit for PCI Bus (2Gb)
IBM xSeries P/N 48P7061	BladeCenter HS20 Fibre Channel Expansion Card
IBM xSeries P/N 48P7062	BladeCenter 2-port Fibre Channel Switch Module
JNI FC64-1063-N	FibreStar 64-Bit SBus Fibre Channel Host Bus Adapter
JNI FCC-6562	FibreStar CompactPCI-to-Fibre Channel Host Bus Adapter (2Gb)
JNI FCC2-6562	FibreStar CompactPCI-to-Fibre Channel Host Bus Adapter (2Gb) (two ports)
JNI FCX-6562	FibreStar PCI-X-to-Fibre Channel Host Bus Adapter (2Gb)
JNI FCX2-6562	FibreStar PCI-X-to-Fibre Channel Host Bus Adapter (2Gb) (two ports)
JNI FCI-1063-N	FibreStar 32-Bit PCI-to-Fibre Channel Host Bus Adapter
JNI FCE-1473-N	FibreStar 2Gb 64-bit SBus-to-Fibre Channel Host Bus Adapter
JNI FCE-6460-N	FibreStar 2Gb 64-bit PCI-to-Fibre Channel Host Bus Adapter
QLogic QCP2340	64-Bit 66MHz PCI 2Gb Fibre Channel Adapter
QLogic QLA2100F	64-Bit PCI-to-Fibre Channel Adapter
QLogic QLA2200F	64-Bit PCI-to-Fibre Channel Adapter (33MHz or 66 MHz)
QLogic QLA2300F	65-Bit PCI-to-Fibre Channel Adapter (66MHz)
QLogic QLA2310F	66MHz PCI-X Fibre Channel Adapter
QLogic QLA2310FL	66MHz PCI-X Fibre Channel Adapter (low profile)
QLogic QLA2340/L	133MHz PCI-X Fibre Channel Adapter (low profile)
QLogic QLA2342/L	133MHz PCI-X Fibre Channel Adapter (two ports; low profile)
SGI PCI-FC-1P-OPT	Optical SW 1GB Fibre Channel Adapter

10.806
RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1242
3698
Doc.

Table 10: Fibre Channel Host Adapters (cont.)

Adapter	Description
SGI PCI-FC-1P-OPT-A	Optical SW 1GB Fibre Channel Adapter
SGI PCI-FC-1POPT-B	Optical SW 2 GB Fibre Channel Adapter
SGI PCX-FC-2POPT-B	Optical SW 2GB Fibre Channel Adapter (two ports)
StorageWorks KGPSA-BC	64-bit / 33 MHz PCI-to-Fibre Channel Host Bus Adapter
StorageWorks KGPSA-CA	64-bit / 33 MHz PCI-to-Fibre Channel Host Bus Adapter
StorageWorks KGPSA-DA	64-bit / 66MHz PCI 2Gb Fibre Channel Adapter
Sun 6727A	64-Bit PCI-to-Fibre Channel Adapter (33MHz or 66 MHz) (dual port)
Sun 6767A	66MHz PCI-X 2Gb Fibre Channel Adapter
Sun 6768A	133MHz PCI-X 2Gb Fibre Channel Adapter (two ports; low profile)
Sun 6799A	64-Bit PCI-to-Fibre Channel Adapter (33MHz or 66 MHz)

Fibre Channel / FICON Intermix

The ESS supports Fibre Channel / FICON intermix on the INRANGE FC/9000 Fibre Channel Director (IBM 2042 Models 001 and 128) and the McDATA ED-6064 (open-open mode) Enterprise Fibre Channel Director (IBM 2032 Model 064). With intermix, both FCP (Fibre Channel Protocol) and FICON upper level protocols can be supported within the same director when deployed independently by port. Cascading of directors is not currently supported with Fibre Channel / FICON intermix.

Fibre Channel / FICON intermix support requires ESS LIC level 1.5.2, or later. Implementation details and operational information for using intermix are available at the INRANGE and McDATA websites.

Table11: SAN Fabric Products

Product	IBM Machine Type and Model or Part Number	Description
Cisco MDS 9216	IBM 2062 Model D01	Cisco Multilayer Fabric Switch (2Gb, 48-port)
Cisco MDS 9509	IBM 2062 Models D07 / T07	Cisco Multilayer Director (2Gb, 224-port)
IBM 2103 Model H07		IBM Fibre Channel Storage Hub
IBM 2109 Model F16	P/N 2109F16	IBM TotalStorage SAN Switch (2Gb, 16-port)
IBM 2109 Model F32	P/N 2109F32	IBM TotalStorage SAN Switch (2Gb, 32-port)
IBM 2109 Model M12		IBM TotalStorage SAN Switch (2Gb, 64-port)
IBM 2109 Model S08	P/N 2109S08	IBM TotalStorage SAN Switch (1Gb, 8-port)
IBM 2109 Model S16	P/N 2109S16	IBM TotalStorage SAN Switch (1Gb, 16-port)
IBM 3534 Model F08	P/N 3534F08	IBM TotalStorage SAN Switch (2Gb, 8-port)
IBM 3534 Model 1RU	P/N 35341RU	IBM TotalStorage SAN Managed Hub
INRANGE FC/9000-64	IBM 2042 Model 001	INRANGE FC/9000 Fibre Channel Director (2Gb, 64-port)
INRANGE FC/9000-128	IBM 2042 Model 128	INRANGE FC/9000 Fibre Channel Director (2Gb, 128-port)
INRANGE FC/9000-256	IBM 2042 Model 256	INRANGE FC/9000 Fibre Channel Director (2Gb, 256-port)
McDATA ES-3016	IBM 2031 Model 016	McDATA ES-3016 Fabric Switch (1Gb, 16-port)
McDATA ES-3032	IBM 2031 Model 032	McDATA ES-3016 Fabric Switch (1Gb, 32-port)
McDATA Sphereon 3216	IBM 2031 Model 216	McDATA Sphereon Fabric Switch (2Gb, 16-port)
McDATA Sphereon 3232	IBM 2031 Model 232	McDATA Sphereon Fabric Switch (2Gb, 32-port)
McDATA Sphereon 4500	IBM 2031 Model 224	McDATA Sphereon Fabric Switch (2Gb, 24-port)
McDATA ED-5000	IBM 2032 Model 001	McDATA ED-5000 Fibre Channel Director
McDATA Intrepid 6064	IBM 2032 Model 064	McDATA Intrepid 6064 Director (2Gb, 64-port)
McDATA Intrepid 6140	IBM 2032 Model 140	McDATA Intrepid 6140 Director (2Gb, 140-port)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1243
3698
Doc.

May 13, 2003

Unless stated otherwise, these items require ESS LIC level 2.2.0, or later, which has a planned availability of June 27, 2003.

ESS Copy Services
- Peer-to-Peer Remote Copy (PPRC) Version 2
- FlashCopy Version 2

Servers
- iSeries 800, 810, 825, and 870
- Sun Fire V120, V280R, and V480
- zSeries 990

Channel Extenders/DWDMs
- Nortel Networks OPTera Metro 5200

Operating Systems, Path Management, and Clustering
- Hewlett Packard OpenVMS 7.3-1
- Hewlett Packard Serviceguard 11.14
- Hewlett Packard Tru64 5.1B
- Sun Cluster 3.0 including MPxIO
- Sun VERITAS Cluster Server 3.5

Operating Systems, Path Management, and Clustering (cont.)
- UnitedLinux 1.0 (Intel): SLES 8 (including CLI and SDD support)
- Windows Server 2003 (including CLI support)
- Windows 2000 Boot Support (including SDD support)
- zSeries VSE/ESA Version 2 Release 7
- zSeries z/VM Version 4 Release 4

Host Adapters
- Emulex LP9802 and LP9402DC (Intel (NetWare, Windows) Sun)
- QLogic QCP2340 (Sun)
- SGI PCI-FC-1POPT-B
- Storage Works KGPSA-DA (HP OpenVMS and Tru64)
- Sun 6727A, 6767A, 6768A, and 6799A.

February 17, 2003

Unless stated otherwise, these items require ESS LIC level 2.1.1, or later, which has a planned availability of February 21, 2003 for the Models 800, F10 and F20.

General
- ESS API: CIM Agent support (AIX, Intel (Linux, Windows 2000)
- SGI Origin Servers

Operating Systems, Path Management, and Clustering
- AIX 5.2 with HACMP 4.5
- Veritas Cluster server for Sun Solaris 9
- Linux (Intel): New kernel levels

Other

End of Service and Support for various Linux/Redhat (Intel) Levels. Refer to the Linux (Intel) server page for specific information.

SAN Fabric
- INRANGE FC/9000-256 (HP, RS/6000, RS/6000 SP, Intel (Linux, Netware, Windows), and Sun)

November 22, 2002

Unless stated otherwise, these items require ESS LIC level 2.1.0, or later, which has a planned availability of November 22, 2002 for the Model 800 and January 31, 2003 for the Models F10 and F20.

General
- Planned availability for ESS Models F10 and F20 interoperability changed to January 31, 2003 for the following items. Additionally ESS LIC level has changed to ESS LIC level 2.1.0 or later.
  - HP rp7410, rp8400, and Superdome
  - HACMP 4.5.0
  - Red Hat Linux 7.2 (Intel)
  - Windows 2000 Datacenter (Intel)
  - SuSE Linux 7.3 (Intel)
  - Sun Fire 12K, and 15K

Servers
- IBM pSeries 650 Model 6M2 and pSeries 655 Model 651
- Sun Fire V880, and 3800

Operating Systems, Path Management, and Clustering
- SuSE Linux Enterprise Server 7 (iSeries)
- AIX 5.2
- Solaris 9

SAN Fabric
- IBM 2109 Model F32 (HP, RS/6000, Intel (Linux, NetWare, Windows), Sun, and NAS)
- McData Sphereon 4500 (HP, RS/6000, Intel (Linux, Netware, Windows), and Sun)
- IBM 2109 Model F16 (NAS)

NAS Fabric
- NAS Gateway 300, Model G27

Adapters
- Emulex LP9002DC (Intel (Linux, Netware, Windows), and Sun)
- JNI FCC-6562 (Sun)

October 22, 2002

Unless stated otherwise, these items require ESS LIC level 2.1.0, or later, which has a planned availability of November 22, 2002 for the Model 800 and January 31, 2003 for the Models F10 and F20

General
- OpenVMS: Fibre Channel support

Configuration Management
- ESS CLI (AIX, HP-UX, Linux (Intel), Solaris, and Windows 2000)

Copy Services CLI
- NetWare 6.0
- OpenVMS

Operating Systems, Path Management, and Clustering
- Linux (Intel): Red Hat Advanced Server 2.1 (including copy services CLI and SDD)
- Linux (Intel): SuSE Linux Enterprise Server 7 (including copy services CLI and SDD)
- NetWare: SDD support

Host Adapters
- Emulex LP9002C (Sun)
- JNI FCC2-6562 and FCX-6562 / FCX2-6562 (Sun)
- QLA2340 / QLA2342L (Linux (Intel), NetWare, and Sun)

Other

Removed footnotes for host adapter restrictions; information has been moved to the Host Bus Adapter Support Matrix.

October 7, 2002

Servers
- IBM iSeries 890

Operating Systems, Path Management, and Clustering
- HACMP 4.5.0
- HP MC/Serviceguard 11.13
- HP-UX 11 (32-bit support for SCSI)

Operating Systems, Path Management, and Clustering (con't)
- OpenVMS 7.2-2
- z/OS and z/OS.e Version1 Release 4

SAN Fabric
- McDATA Intrepid 6140 (HP, IBM pSeries, Intel (Linux, NetWare, Windows), and Sun

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1244
3698
Doc.

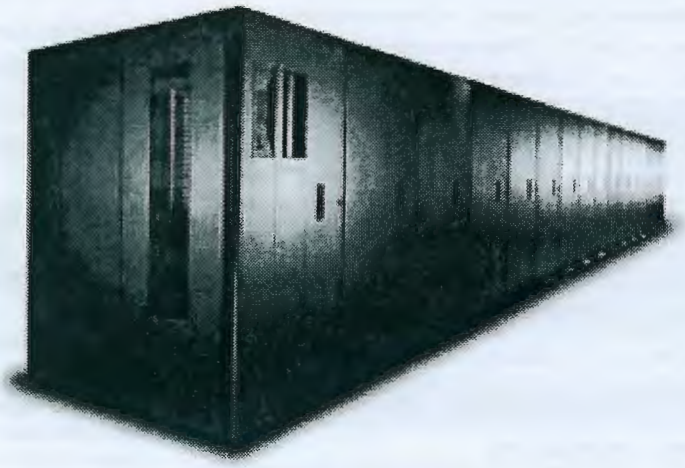
Manual 05

IBM TotalStorage TM
UltraScalable Tape Library 3584

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1245
Doc. 3698

An UltraScalable, ultra-flexible tape library for backup and archival solutions

IBM TotalStorage™ UltraScalable Tape Library 3584



IBM TotalStorage UltraScalable Tape Library 3584 with 16 frames

Highlights

- ***Offers 16-frame capacity, performance, and reliability for midrange and network tape storage environments***
- ***Provides an UltraScalable solution to help protect your technology investment***
- ***Patented Multi-path Architecture helps increase configuration flexibility with logical library partitioning***
- ***Adheres to widely supported Linear Tape-Open™ (LTO) Ultrium™ design specifications***
- ***Offers native switched fabric 2Gb Fibre Channel LTO Ultrium 2 Drives***

IBM TotalStorage UltraScalable Tape Library—A flexible solution

From midrange systems to large-scale server-based operations, the IBM TotalStorage UltraScalable Tape Library is designed to handle backup, archive, and disaster recovery data storage needs with ease.

Advanced features

The IBM TotalStorage UltraScalable Tape Library 3584 now supports up to 16 frames housing a maximum of 6,881 tape cartridges and 192 Ultrium tape drives. Support for the IBM TotalStorage Ultrium 2 Tape Drive more than doubles tape drive performance over the first generation LTO Ultrium Tape Drive and is designed to support up to 35MB/sec native data transfer rates (70MB/sec with 2:1 compression). In addition, with the use of the new IBM TotalStorage LTO Ultrium 200GB Data Cartridge, the IBM TotalStorage Ultrium 2 Tape Drive doubles the tape cartridge capacity up to 200GB native capacity (400GB with 2:1 compression).

The IBM TotalStorage Ultrium 2 Tape Drives can read and write original LTO Ultrium data cartridges at first generation Ultrium 1 capacities with improved performance. The Ultrium 2 tape drives and cartridges can be resident in the same 3584 Library frame with first generation Ultrium tape drives and Cartridges. The UltraScalable Tape Library is designed with a variety of advanced features. IBM's Multi-path Architecture is designed to simultaneously attach heterogeneous servers and applications to LTO logical library partitions, including mixed Ultrium drives and media.

Remote management capabilities using a Web browser provides library control and configuration. Simple Network Management Protocol (SNMP) functionality is also included. Hot swap drives, data path failover and load balancing and redundant power supplies offer enhanced availability. New control path failover for AIX, dual AC power and 110 volt power options are also available.

Software support

You can maximize the power of the UltraScalable Tape Library by managing it with industry-leading tape management solutions such as Tivoli®

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1246
Doc. 3698

IBM TotalStorage UltraScalable Tape Library 3584 at a glance

Model number	L32—LTO base frame; D32—LTO expansion frame

Characteristics

Tape drive type	IBM LTO Ultrium 2 or 1
Number of frames	One base frame and up to 15 expansion frames
Number of drives	Up to 192: L32—1 to 12 LTO; D32—0 to 12 LTO
Number of tape cartridges	Up to 6,881: L32—87 to 281; D32—396 to 440
Number of logical libraries	Up to 192: L32—up to 12; D32—up to 12
Capacity[1,2]	2,752 TB compressed, in a 16-frame configuration with four drives L32 (1-4 drives)—Up to 112.4 TB/frame compressed; 56.2 TB native D32 (0 drives)—Up to 176 TB/frame compressed; 88.0 TB native
Sustained data transfer rate[2]	LTO Ultrium 2: Up to 70 MB/sec compressed; 35 MB/sec native
Measured aggregate sustained data rate[2]	Up to 47.4 TB/hour with 192 LTO Ultrium 2 tape drives (compressed)[2]
Media type	IBM TotalStorage LTO Ultrium 200 GB Data Cartridge (P/N 08L9870) IBM TotalStorage LTO Cleaning Cartridge (P/N 35L2086)
Dimensions (L32 or D32)	70.9" H x 28.5" W x 59.8" D (1800 mm x 725 mm x 1520 mm)
Max. weight	L32—1236.0 lb (539.4 kg); D32—1161.9 lb (527.0 kg)
Warranty	One year; IBM On-site Repair (IOR)

Operating environment

Temperature	16° to 32° C (60.8° to 89.6° F)
Relative humidity	20% to 80% (non-condensing)
Wet bulb maximum	23.0° C (73.4° F)
Electrical power	8 amps at 200-240 VAC; 1.6 kVA, 1.4 kilowatt nominal 12 amps at 100-127 VAC; 1.2kVA, 1.2 Kilowatt nominal
Noise level	7.5 bels; 51 dBA operating

Attachment and systems support[3]

The IBM 3584 features LTO Fibre Channel, LVD Ultra2/Wide or Ultra160 SCSI and HVD Ultra SCSI interfaces, attaching to IBM @server pSeries™, IBM @server iSeries™, IBM @server xSeries™, RS/6000®, RS/6000 SP, AS/400®, and Netfinity® systems, and non-IBM servers and workstations

Operating systems support[3]

Device driver support is available for AIX®; OS/400®; Windows NT®; Windows® 2000; Windows 2003; Sun Solaris; and HP-UX.

[1] Capacity depends on the number of drives installed versus the number of tape cartridges used
[2] Based on 2:1 compression
[3] For latest information, consult Technical Support at www.ibm.com/totalstorage/lto

Storage Manager or other storage software.

Why IBM LTO?

IBM LTO Ultrium drives share best-of-breed technology. Advanced multi-track recording capabilities, state-of-the-art magneto-resistive (MR) heads, and a sophisticated track following servo system work together to produce extremely high recording densities.

New Ultrium 2 drive enhancements include digital speed matching, power management, channel calibration and 512 data tracks. Error correction code (ECC) function and Statistical Analysis and Reporting System (SARS) help support data integrity.

For more information

For more information, contact your IBM representative or your IBM Business Partner. For updated attachment, supported operating system, media product, and storage management software information, visit www.ibm.com/totalstorage/lto.

© International Business Machines Corporation 2003

IBM Systems Group
Removable Media Storage Solutions
9000 S. Rita Road
Tucson, AZ 85744
United States

Produced in the United States
06-03
All Rights Reserved

IBM, AIX, AS/400, @server, iSeries, Netfinity, OS/400, pSeries, RS/6000, and xSeries, are registered trademarks of International Business Machines Corporation.

Linear Tape-Open, LTO, the LTO logo, Ultrium, and the Ultrium logo are U.S. trademarks of HP, IBM, and Seagate. Tivoli is a registered trademark of Tivoli Systems, Inc. DLT tape is a registered trademark of Quantum. Windows and Windows NT are registered trademarks of Microsoft Corporation. Other company, product, and service names may be trademarks or registered trademarks of their respective companies.

Other company, product, and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

Product data is accurate as of initial publication and is subject to change without notice.

Photography depicts design models. Actual product may show slight variations.

G225-6853-05

10.798
1

Manual 06

The IBM LTO Ultrium Tape Libraries Guide
(REDBOOK)

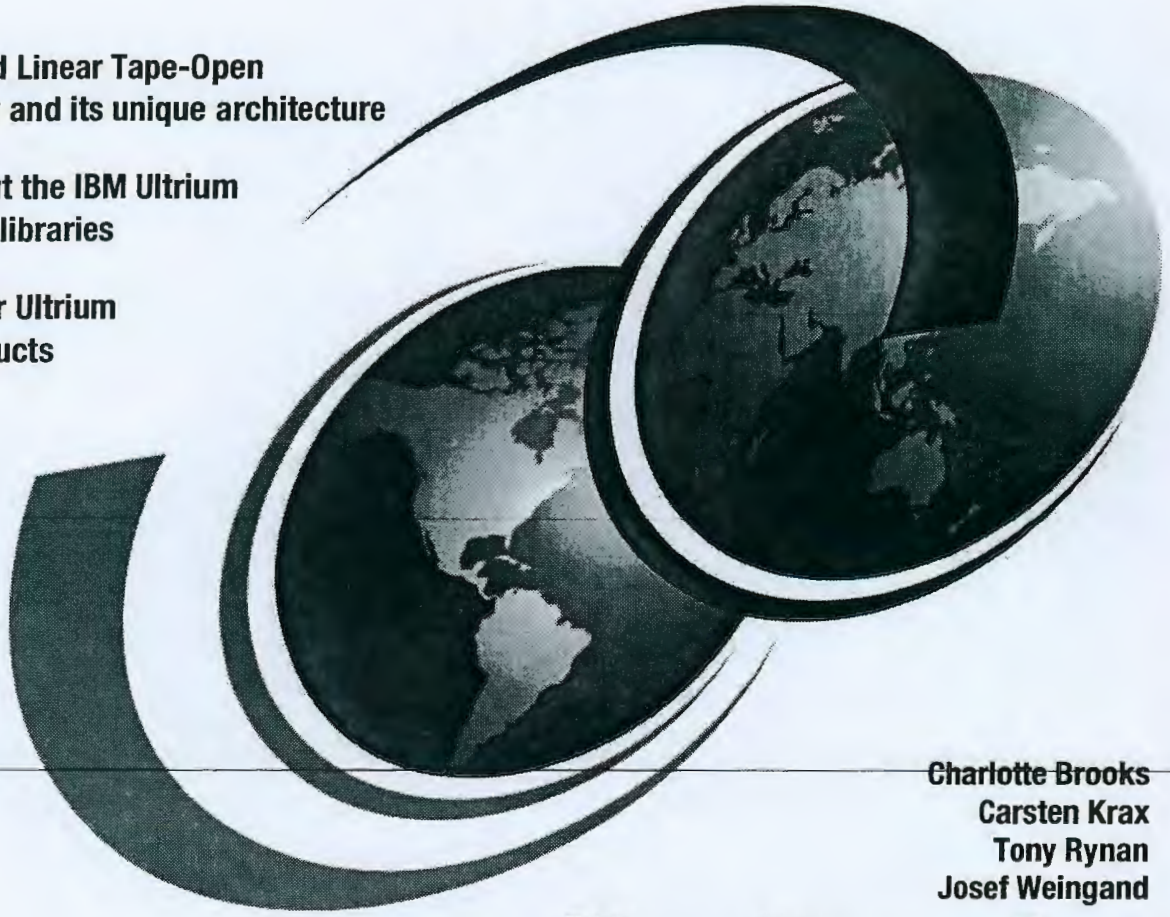
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1247
Doc. 3698

10.797

IBM

The IBM LTO Ultrium Tape Libraries Guide

- Understand Linear Tape-Open technology and its unique architecture
- Learn about the IBM Ultrium drives and libraries
- Updated for Ultrium LTO 2 products



Charlotte Brooks
Carsten Krax
Tony Rynan
Josef Weingand

Redbooks

ibm.com/redbooks

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1248
3698
Doc.

10796
1

IBM International Technical Support Organization

The IBM LTO Ultrium Tape Libraries Guide

June 2003

SG24-5946-01

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1249
Doc. 3698

10.795

Note: Before using this information and the product it supports, read the information in "Notices" on page xvii.

Second Edition (June 2003)

This edition applies to the IBM TotalStorage Ultrium Tape Drive 3580, IBM TotalStorage Ultrium Tape Autoloader 3581, IBM TotalStorage Ultrium Tape Library 3582, IBM TotalStorage Ultrium Scalable Tape Library 3583, and IBM TotalStorage UltraScalable Tape Library 3584.

© Copyright International Business Machines Corporation 2000, 2003. All rights reserved.
Note to U.S. Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures xi

Tables xv

Notices xvii
Trademarks xviii

Preface xix
The team that wrote this redbook. xix
Become a published author xxi
Comments welcome. xxii

Summary of changes xxiii
June 2003, Second Edition xxiii

Chapter 1. Introduction to Linear Tape-Open (LTO) 1
1.1 The LTO organization 2
1.1.1 Open licensing and manufacture 3
1.1.2 License packages 4
1.1.3 Compliance verification 5
1.2 LTO standards. 5
1.2.1 Ultrium tape formats 5
1.2.2 LTO core technology. 6

Chapter 2. LTO technology 9
2.1 Interleaved recording. 10
2.1.1 Servo tracks 10
2.1.2 Data tracks 13
2.1.3 Linear density 16
2.2 Data compression 16
2.3 Tape cartridge 18
2.3.1 Metal particle medium 20
2.3.2 Cartridge memory (LTO-CM) 20
2.3.3 Barcode label 22
2.3.4 Volume label format 23
2.3.5 Write protect switch. 24
2.3.6 Cleaning the cartridge 24
2.3.7 Cartridge life 24
2.3.8 Cleaning cartridge 25

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1250
Fls Nº 3698
Doc.

0793

2.3.9 Cartridge handling 25
2.4 IBM LTO Ultrium common subassembly 28
2.4.1 Drive head 29
2.4.2 Data compression 30
2.4.3 Interfaces 31
2.4.4 Performance 35
2.4.5 Partial Response Maximum Likelihood (PRML) 36
2.4.6 IBM Ultrium 2: additional improvements 37
2.4.7 IBM Ultrium 1 and 2 compatibility 39
2.4.8 Operating the Ultrium drive 39
2.4.9 Reliability 41
2.4.10 Cleaning the drive 43
2.5 The IBM LTO Ultrium family of tapes and libraries 44
2.6 Multi-path architecture 46

Chapter 3. Tape storage market direction 49
3.1 Current tape products and technologies 50
3.1.1 Helical versus longitudinal 50
3.1.2 Tape reels (1/2-inch) 52
3.1.3 QIC 52
3.1.4 Digital Data Standard (4 mm) 54
3.1.5 The 8 mm format 56
3.1.6 Digital Linear Tape (DLT) 58
3.1.7 SuperDLT (SDLT) 62
3.1.8 IBM 3480 63
3.1.9 IBM 3490 63
3.1.10 IBM Magstar 3590 64
3.1.11 STK 9840 65
3.1.12 STK 9940 66
3.1.13 LTO Ultrium 66
3.1.14 Libraries 67
3.2 Current SAN technologies 68
3.2.1 SAN definition 70
3.2.2 Fibre Channel architecture 70
3.2.3 Topologies 71
3.2.4 Tape solutions in a SAN environment 71

Chapter 4. IBM TotalStorage Ultrium Tape Drive 3580 79
4.1 Model description 80
4.2 Feature codes 81
4.3 SCSI attachment 82
4.4 SCSI cabling 82
4.4.1 Cables 82

10.792

4.4.2 Interposers 83
4.4.3 SCSI length limitations 83
4.5 Upgrades 84
4.6 Environmental specifications 84
4.6.1 Physical dimensions 84
4.6.2 Operating environment 84
4.7 Host platforms and device drivers 84
4.7.1 Device driver installation 85
4.8 Storage applications 86
4.9 Performance considerations 86
4.10 Media 87
4.11 IBM 3580 Ultrium tape drive initial set-up 87
4.11.1 SCSI ID 87
4.12 Operator displays and buttons 88
4.12.1 Status light 88
4.12.2 Message display 89
4.12.3 The single-character display 89
4.12.4 Unload push button 90
4.13 Drive cleaning 90
4.14 Firmware upgrade 91

Chapter 5. IBM TotalStorage Ultrium Tape Autoloader 3581 93
5.1 Model description 95
5.1.1 Feature codes 96
5.1.2 Access mode 96
5.1.3 SCSI devices 97
5.1.4 Adding and removing cartridges 97
5.1.5 Operation 98
5.2 SCSI attachments 98
5.3 SCSI cabling 98
5.3.1 Cables 99
5.3.2 Interposers 99
5.3.3 SCSI length limitations 100
5.4 Upgrades and optional features 100
5.5 Environmental specifications 101
5.5.1 Physical dimensions 101
5.5.2 Operating environment 101
5.6 Host platforms and device drivers 101
5.6.1 Device driver installation 102
5.7 Storage applications 103
5.8 Performance considerations 103
5.9 Media 103
5.10 IBM 3581 initial setup 104

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1251
Doc. 3698

5.10.1 SCSI ID 104
5.10.2 Element numbers 105
5.10.3 Operator displays and buttons 105
5.10.4 Message display 106
5.10.5 Drive status messages 107
5.10.6 Control buttons 108
5.10.7 Operating modes. 110
5.11 Drive cleaning 111
5.12 Firmware upgrade 112

Chapter 6. IBM TotalStorage Ultrium Tape Library 3582 113
6.1 Model description 114
6.1.1 Tape drives 115
6.1.2 Cartridge storage 115
6.1.3 Barcode scanner 117
6.1.4 I/O station 117
6.1.5 Robotic system 117
6.1.6 Library control and operation 117
6.1.7 Operator panel 118
6.1.8 Maintenance 118
6.2 Feature codes 118
6.3 Physical attachments 119
6.4 SCSI cabling 120
6.4.1 Cables 120
6.4.2 Interposers 121
6.4.3 SCSI length limitations 121
6.5 Environmental specifications. 121
6.6 Host platforms and device drivers. 121
6.6.1 Device driver installation 122
6.7 Storage applications 123
6.8 Media. 123
6.9 Installation and performance considerations. 124
6.10 IBM 3582 initial set-up. 124
6.10.1 SCSI ID 125
6.10.2 Identifying library location element numbers. 125
6.11 Operator displays and buttons 125
6.11.1 Operator Panel 126
6.12 Library mode 128
6.13 Drive cleaning 128
6.14 Firmware upgrades 128

Chapter 7. IBM TotalStorage Ultrium Scalable Tape Library 3583 129
7.1 Model description 131

7.1.1 Tape drives 131
7.1.2 Cartridge storage 132
7.1.3 Barcode reader 132
7.1.4 I/O station 133
7.1.5 Robotic system 133
7.1.6 Library control and operation 133
7.1.7 Operator panel 134
7.1.8 Remote Management Unit 134
7.1.9 Library partitioning 134
7.1.10 Multiple control paths 135
7.1.11 SAN Data Gateway Module 135
7.1.12 Maintenance 135
7.2 Feature codes 136
7.3 Physical attachments 137
7.4 Cabling 138
7.4.1 Fibre Channel cables 138
7.4.2 SCSI cables 139
7.4.3 Interposers 140
7.4.4 Terminator 140
7.4.5 Cable length limitations 140
7.5 Upgrades and optional features 141
7.5.1 Upgrade features 141
7.5.2 Optional features 142
7.6 Environmental specifications 142
7.7 Host platforms and device drivers 143
7.7.1 Device driver installation 144
7.8 Storage applications 144
7.9 Media 145
7.10 Installation and performance considerations 145
7.11 IBM 3583 initial set-up 146
7.11.1 SCSI ID and LUN assignment 146
7.11.2 Identifying library locations 147
7.11.3 Element numbers 150
7.12 Operator panel and RMU 151
7.12.1 Operator panel 151
7.12.2 RMU with TotalStorage Specialist 154
7.13 Random access 156
7.14 Drive cleaning 156
7.15 Firmware upgrades 157

Chapter 8. IBM TotalStorage UltraScalable Tape Library 3584 159
8.1 Model description 161
8.1.1 IBM 3584 Library Unit L32 161

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1252
Doc. 3698

8.1.2 IBM 3584 Expansion Unit D32 163
8.2 Library components 165
8.2.1 Tape drives 165
8.2.2 Library control systems: frame control assembly 167
8.2.3 Operator interface 170
8.2.4 Robotic cartridge accessor 172
8.2.5 Rail assembly 174
8.2.6 Library centric WWN convention 174
8.2.7 Control path failover 175
8.2.8 StorWatch 176
8.2.9 I/O station 177
8.2.10 Reliability 177
8.2.11 Service 179
8.2.12 Capacity 181
8.2.13 Adding and removing cartridges 185
8.3 Performance 186
8.4 Upgrades and optional features 188
8.4.1 Upgrade features 188
8.4.2 Optional features 189
8.5 Environmental specifications 189
8.5.1 Physical dimensions 189
8.5.2 Floor requirements 190
8.5.3 Operating environment 191
8.5.4 Power and cooling specifications 191
8.6 Host platforms and device drivers 192
8.6.1 Device driver installation 193
8.7 Storage applications 193
8.8 IBM 3584 initial setup 194
8.8.1 SCSI ID 194
8.8.2 Element number 194
8.9 Operator displays and buttons 196
8.10 Sequential versus random access 198

Chapter 9. IBM xSeries LTO tape products 199
9.1 IBM 3607-26X and 4560-SLX 200
9.1.1 Tape drives 202
9.1.2 Barcode reader 202
9.1.3 I/O station 202
9.1.4 Robotic system 203
9.1.5 Library control and operation 203
9.1.6 Operator panel 204
9.1.7 Maintenance 204
9.2 Library options 204

9.3 Physical attachments 205
9.4 Cabling 205
9.5 Environmental specifications 206
9.6 Storage applications 206
9.7 Media 206
9.8 Installation and performance considerations 207
9.9 Library features 207
9.9.1 Identifying library locations element numbers 207
9.10 Operator displays and buttons 208
9.10.1 Operator panels 208
9.10.2 Menu options 210
9.11 Library modes 210
9.12 Drive cleaning 210
9.13 Firmware upgrades 210

Chapter 10. LTO and iSeries considerations 213
10.1 iSeries support for IBM LTO Ultrium 2 214
10.2 BRMS and LTO tape libraries 215
10.3 iSeries resources 216
10.3.1 Configuration changes 218
10.4 OS/400 V5R1 restriction for multi-path architecture libraries 218
10.5 OS/400 V5R2 218
10.6 Tape drive sharing and management 220

Appendix A. LTO Ultrium tape media 223
Features available with IBM LTO hardware initial order 225
IBM TotalStorage Ultrium 1 Tape Drive 3580 225
IBM TotalStorage Ultrium 2 Tape Drive 3580 225
IBM TotalStorage Ultrium Tape Library 3582 225
IBM TotalStorage Ultrium 1 Scalable Tape Library 3583 226
IBM TotalStorage Ultrium 2 Scalable Tape Library 3583 227
IBM TotalStorage Ultrium 1 UltraScalable Tape Library 3584 227
IBM TotalStorage Ultrium 2 UltraScalable Tape Library 3584 228
IBM 3589 Ultrium 1 tape cartridge model number 228
Model description 229
Labelling service 229
IBM media business distributors and other suppliers 231

Abbreviations and acronyms 233

Related publications 235
IBM Redbooks 235
Other publications 235
Online resources 236

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1253
Doc. 3698

How to get IBM Redbooks 237

Index 239

Figures

1-1 LTO Ultrium roadmap 2
1-2 LTO trademarks 5
1-3 IBM LTO Ultrium 1 and Ultrium 2 tape cartridges 6
2-1 Servo band position and nomenclature 11
2-2 Magnified servo band showing a pair of servo bursts 12
2-3 Encoding bits using the servo stripes within the servo bursts 13
2-4 Four data bands written between the servo tracks 14
2-5 Portion of data band showing Ultrium 1 track-writing sequence 15
2-6 LTO-DC block diagram 16
2-7 Ultrium cartridge view from top and rear 18
2-8 Ultrium cartridge view from top and front 19
2-9 Leader pin attached to the tape medium 20
2-10 Barcode label example 22
2-11 Turtle case 26
2-12 Double box 27
2-13 Correct leader pin placement 27
2-14 IBM LTO Ultrium common subassembly 28
2-15 Eight-element head (one set of heads shown) and servo elements . . . 29
2-16 Allocation of read and write heads for forward and reverse wrap 30
2-17 HD68 connector 34
2-18 VHDCI connector 34
2-19 IBM linear implementation of PRML encoding 37
2-20 Speed matching comparison: MB/sec 38
2-21 IBM Ultrium 1 and 2 compatibility 39
2-22 Front of subassembly showing operator panel indicators 40
2-23 Surface control guiding 42
2-24 Flat lap head 42
2-25 Statistical Analysis and Reporting System 43
2-26 The IBM Ultrium family of tapes and libraries 44
2-27 Conventional tape library vs. multi-path architecture 46
2-28 Redundant control paths to the library controller 47
2-29 IBM LTO tape library partitioned into three logical libraries 48
3-1 Tape reels, 1/2-inch 52
3-2 QIC cartridge 53
3-3 QIC head diagram 54
3-4 Helical-scan recording diagram 55
3-5 An 8 mm tape path 57
3-6 DLT tape path mechanism 59

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1254
Doc. 3698

3-7 DLT 2000 recording head design 60
3-8 DLT cartridge 60
3-9 DLT 2000/4000 linear recording format 61
3-10 DLT 7000/8000 tape head 61
3-11 Symmetric Phase Recording technology 61
3-12 Magstar 3590 tape cartridge 64
3-13 Magstar 3590 tape drive 65
3-14 STK 9840 tape cartridge 66
3-15 Overview of a SAN 69
3-16 IBM 3584 multi-path architecture 73
3-17 Electronic vaulting 75
3-18 Tivoli Storage Manager LAN-free backup 76
3-19 Tivoli Storage Manager server-free backup 77
4-1 IBM 3580 model L11/L13/L23 or H11/H13/H23 Ultrium tape drive 80
4-2 SCSI ID set-up example 88
4-3 Front view of the IBM 3580 tape drive 90
5-1 IBM TotalStorage Ultrium Tape Autoloader 3581 95
5-2 IBM 3581 cartridge slots 97
5-3 IBM 3581 front view 106
5-4 IBM 3581 message display 107
5-5 IBM 3581 operator panel 109
6-1 IBM TotalStorage Ultrium Tape Library 3582 114
6-2 IBM 3582 seven-slot magazines 116
6-3 IBM 3582 rear-mounted storage slots 116
6-4 IBM 3582 operator panel 126
6-5 IBM 3582 top-level menu options 127
7-1 IBM TotalStorage Ultrium Scalable Tape Library 3583 130
7-2 IBM 3583 storage columns: top view 148
7-3 IBM 3583-L72 location logical view 149
7-4 IBM 3583 front view, open door 150
7-5 IBM 3583 tape library operator panel 152
7-6 IBM 3583 flowchart of library functions 153
7-7 IBM 3583 soft key symbols 154
7-8 IBM 3583 operator panel: input field 154
7-9 IBM 3583 TotalStorage Specialist Web interface 156
8-1 IBM 3584 UltraScalable tape library L32 160
8-2 IBM 3584-L32 base frame view from front left 162
8-3 IBM 3584-D32 library expansion frame viewed from the right 163
8-4 IBM 3584 with 16 frames 164
8-5 IBM 3584 library showing the major library components 165
8-6 IBM 3584 LTO Ultrium tape drive assembly 166
8-7 Redundant drive power supply 167
8-8 IBM 3584 distributed control system 167

8-9 IBM 3584 distributed control system 168
8-10 Redundant medium changer controller 169
8-11 Frame controller assembly. 170
8-12 Operator panel 171
8-13 IBM 3584 accessor assembly 172
8-14 IBM 3584 Gripper. 173
8-15 Drive WWNs of an IBM 3584 175
8-16 Redundant control paths to the library controller 176
8-17 IBM 3584-L32 base frame showing cartridge slot components 182
8-18 IBM 3584-D32 expansion frame showing slot components. 184
8-19 IBM 3584-L32 operator display 197
9-1 IBM 3607-26X Autoloader 200
9-2 IBM 4560-SLX Modular Tape Library 201
9-3 3607-26X front panel 208
9-4 4560-SLX touch screen front panel 209
10-1 Multiple-target support 219

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1255
3698
Doc.

10783

Tables

2-1 Data fields stored in the LTO-CM 21
2-2 SCSI terms and characteristics 33
3-1 Tape technology overview 51
3-2 DDS standards. 56
3-3 Standards for 8 mm 58
3-4 DLT drive standards. 62
4-1 IBM 3580 feature codes. 81
5-1 IBM 3581 feature codes. 96
5-2 IBM 3581 element numbers. 105
6-1 IBM 3582 model summary 115
6-2 IBM 3582 feature codes. 118
6-3 IBM 3582 element numbering 125
7-1 IBM 3583 model summary 131
7-2 IBM 3583 feature codes. 136
7-3 IBM 3583 capacity upgrades 142
7-4 IBM 3583 storage slot coordinates 147
7-5 IBM 3583 element numbering 150
8-1 IBM 3584-L32 slot capacity without capacity expansion feature 183
8-2 IBM 3584-L32 slot capacity with capacity expansion feature 183
8-3 IBM 3584-D32 cartridge slot capacity 185
8-4 IBM 3584 bandwidth 187
8-5 Library performance. 187
8-6 Power requirements for the IBM 3584 192
8-7 IBM 3584 tape drive element numbers 195
9-1 3607-26X Autoloader model summary 200
9-2 4560-SLX Modular Tape Library with Ultrium 1 drives 201
9-3 IBM 4560-SLX options 204
9-4 IBM 4560-SLX element numbering 207
9-5 IBM 3607-26X element numbering 208
9-6 Library manuals 211
A-1 Maximum number of media features for IBM 3583 Ultrium 1 226
A-2 Maximum number of media features for IBM 3583 Ultrium 2 227
A-3 Maximum number of media features for IBM 3584 Ultrium 1 228
A-4 Maximum number of media features for IBM 3584 Ultrium 2 228
A-5 Color specify feature codes for the IBM 3589 model 002 231
A-6 LTO Ultrium 1 and 2 available supplies and part numbers 231

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1256
3698
Doc.

10.782
J

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1257
Doc. 3698

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
AS/400®
DFSMS/MVS®
DFSMShsm™
DFSMSrmm™
ESCON®
@server ™
@server™
FICON™
IBM®
ibm.com®
iSeries™
Magstar®
MVS™
Netfinity®
NetView®
OS/400®
pSeries™
Redbooks™
Redbooks (logo) ™
RS/6000®
ServerProven®
StorWatch™
Tivoli®
TotalStorage®
xSeries™

The following terms are trademarks of other companies:

Intel, Intel Inside(logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM Redbook presents a general introduction to Linear Tape-Open (LTO) technology and the implementation of corresponding IBM® products. As such it describes both general LTO technology specification and specific details of the unique design of IBM Ultrium tape drives and libraries.

In addition to the description of LTO, the reader will find technical information about each of the IBM Ultrium products, including generalized sections about SCSI and Fibre Channel connections, multi-path architecture configurations, and tape technology comparisons with market positioning.

This book is intended for anyone who would like to understand more about the general LTO technology specification and how it came about, as well as the IBM implementation of that specification. It is suitable for IBM clients, business partners, IBM specialist sales representatives, and technical specialists. Those with no background in computer tape storage products may need to reference other sources of information; in the interest of being concise, topics that are generally understood (in the opinion of the writers) are not covered in detail.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Charlotte Brooks is an IBM Certified IT Specialist and Project Manager for Storage Solutions at the International Technical Support Organization, San Jose Center. She has 13 years of experience with IBM in the fields of Storage, pSeries™ and AIX®. She has written 11 Redbooks™ and has developed and taught IBM classes on all areas of storage management. Before joining the ITSO in 2000, she was the Technical Support Manager for Tivoli® Storage Manager in the Asia Pacific region.

Carsten Krax is a Storage Specialist with the IBM Systems Sales Organization in Germany. He provides technical sales support for Open Systems Disk, Tape, and SAN solutions. Before he joined IBM two years ago, he worked from 1995 to 1998 as an System Administrator for an IBM Customer and from 1999 to 2001 as an ADSM/TSM and Storage Specialist for an IBM Business Partner. He holds a Diplom-Ingenieur (FH) degree in Electrical Engineering from the University of Applied Sciences in Dortmund, Germany.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1258
Doc. 3698

30.749

Tony Rynan is a senior software specialist at IBM Australia. He currently performs architectural and implementation services for IBM Global Services Australia throughout Southeast Asia. His areas of expertise include Tivoli Storage Manager, pSeries, SP, and SAN. He co-authored the redbook *Implementing IBM LTO in Linux and Windows*, SG24-6268.

Josef Weingand is an IT Specialist with the IBM Systems Sales Organization in Germany. He has seven years of experience providing technical support in IBM. He started as a customer engineer for Large Systems and worked 2 1/2 years as a Team Leader for the ITS European Support Center for Optical, Tape, and Tape Libraries. Now he is providing technical sales support for tape and backup solutions. He holds a Diplom-Ingenieur (FH) degree in Electronic Engineering from the Fachhochschule Kempten. He co-authored the Redbook *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

The team: Tony, Josef, Charlotte, and Carsten

Thanks to the following people for their contributions to this project:

The authors of the first edition of this book: Matthias Werner, Christina Coutts, Michel Marion, and Nelson Saavedra

10.748

Jon Tate, Emma Jacobs, Deanna Polm
International Technical Support Organization, San Jose Center

Betsy Thaggard
International Technical Support Organization, Austin Center

Nancy Coon, John Latimore, Dan Watanabe
IBM Tape Marketing, Tucson

Bob Bingham, Bobby Bohuslav, Michael DeGon, Brian Goodman, Lee Jesionowski, Dave Minch, Yun Mou, Steve Nunn, Bob O'Connell, Carol Pilch, MT Rincon, Robin Roberts, Carla Ruhl, John Sellars, Rob Wilson, Ray Yardy,
IBM Tape Architecture, Development, and Testing, Tucson

Rajesh Gurjar
IBM Systems Group, San Jose

Jo Lay
IBM Tivoli Storage Management Development, San Jose

Nancy Roper,
IBM iSeries™ Advanced Technical Support, Markham

Scott Maxson,
IBM iSeries Development, Rochester

David Turner,
IBM xSeries™ Tape Marketing, Raleigh

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1259
Doc. 3698

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  `ibm.com/redbooks`

- Send your comments in an Internet note to:

  `redbook@us.ibm.com`

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. QXXE Building 80-E2
  650 Harry Road
  San Jose, California 95120-6099

Summary of changes

This section describes the technical changes made in this edition of the book and in previous editions. This edition may also include minor corrections and editorial changes that are not identified.

Summary of Changes for *The IBM LTO Ultrium Tape Libraries Guide*, SG24-5946-01, as updated on June 9, 2003.

June 2003, Second Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

- Ultrium 2 drives in existing LTO libraries
- New model, IBM® TotalStorage® Ultrium Tape Library 3582
- New functions (multi-path architecture, control path failover) for LTO libraries

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1260
Doc. 3698

10.745
J

1

Introduction to Linear Tape-Open (LTO)

The Linear Tape-Open (LTO) program is a joint initiative of IBM, Hewlett-Packard, and Seagate Technology. In 1997, the three technology provider companies set out to enable the development of best-of-breed tape storage products by consolidating state-of-the-art technologies from numerous sources, and in November of that year they produced a joint press release about LTO.

In the tape storage industry, Hewlett-Packard, IBM, and Seagate saw a common set of problems affecting customers in the midrange and network server areas. Multiple tape options are available, each offering certain strengths in terms of capacity, performance, data integrity, reliability, and cost, but no single option appears to meet all of these customer needs effectively. The LTO technology objective, therefore, was to establish new open-format specifications for high-capacity, high-performance tape storage products for use in the midrange and network server computing environments, and to enable superior tape product options.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1261
Doc. 3698

1.1 The LTO organization

The two principal Web sites for marketing, technical, and licensing detail for the Linear Tape Open program are

`http://www.lto-technology.com`
`http://www.ultrium.com`

Two LTO formats (Ultrium and Accelis) were originally introduced in 1997, and licenses for the new technology were made available. Since then, the Accelis format has not been actively pursued by manufacturers because it is apparent that the Ultrium format meets market needs. The three LTO sponsoring companies (IBM, Hewlett-Packard, and Seagate) also took steps to protect customer investment by providing a four-generation roadmap, shown in Figure 1-1, and establishing an infrastructure to enable compatibility between products. At the time of writing, LTO generations 1 and 2 are available.

LTO Ultrium Road Map

	Generation 1	Generation 2	Generation 3	Generation 4
Capacity (Native)	100GB	200GB	400GB	800GB
Transfer Rate (Native)	10-20MB/s	20-40MB/s	40-80MB/s	80-160MB/s
Media	Metal Particle	Metal Particle	Metal Particle	Thin Film

Figure 1-1 LTO Ultrium roadmap

Important: Hewlett-Packard, IBM, and Seagate reserve the right to change the information in this migration path without notice.

The LTO Ultrium compatibility investment protection is provided based on the following principles:

- An Ultrium drive is expected to read data from a cartridge in its own generation and at least the two prior generations.

10743

– An Ultrium drive is expected to write data to a cartridge in its own generation and to a cartridge from the immediate prior generation in the prior generation format.

Existing compatibility between the available Ultrium 1 and Ultrium 2 media is discussed in 2.4.7, "IBM Ultrium 1 and 2 compatibility" on page 39.

The three technology provider companies (HP, IBM, and Seagate) have all made significant contributions of time and expertise to the definition of the LTO format specifications. All have deep knowledge of customer needs and have provided expert knowledge and engineering skill in the critical areas of magnetic recording technology, mechanism design, media materials, and cartridge design. This cooperative process has created stronger LTO format definitions than any of the individual companies would have developed working alone.

1.1.1 Open licensing and manufacture

To answer industry calls for open tape format specifications, LTO format specifications have been made available to all who wish to participate through standard licensing provisions. More than 25 companies, including HP, IBM, and Seagate, have become LTO technology licensees. The licensees include an impressive array of worldwide storage industry leaders such as:

- Accutronics Inc.
- ADIC
- Advanced Research Corp.
- Alps Electric Co. Ltd.
- Certance
- EDP/Colorflex
- EMag Solutions
- EMTEC Magnetics GmbH
- Exabyte Corporation
- Fuji Photo Film Company Ltd.
- Fujitsu Ltd./FCPA Intellistor
- Hewlett-Packard Co.
- Hi/fn
- IBM Corp.
- Imation Corp.
- M4 Data Ltd.
- Matsushita Electric Industry
- Maxwell
- Mitsumi Electric Co. Ltd.
- Mountain Engineering II Inc.
- NEC Corp.
- Otari Inc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1262
Doc. 3698

- Ontrack Data International
- Overland Data, Inc.
- Phillips Semiconductor Gratkorn
- Plasmon IDE Inc.
- Quantegy Inc.
- Seagate Corporation
- Sony Corp.
- Tandberg Data
- TDK Corp.
- Verbatim Corp.

In attracting these other industry leading companies, LTO program technology and LTO specified products (tape drives and tape storage cartridges) will reach the market from multiple manufacturers, not just the technology provider companies. This is critical to meeting an open market objective and is accomplished through open licensing of the technology.

1.1.2 License packages

Three combinations of packages are available for potential licensees:

- *Ultrium Specification Document* provides the opportunity to review Ultrium format specification with a minimal investment and is suitable for those companies interested in a feasibility investigation.
- *Ultrium Tape Cartridge License Package* is for those companies interested only in designing Ultrium tape cartridges.
- *Ultrium Tape Mechanism License Package* enables the licensee to design Ultrium tape drive mechanisms.

Each license package contains one or all of the following types of documents:

- *Format specification documentation*, which provides the technical information about the format necessary to develop mechanisms and cartridges that interchange between products of the same format.
- *License documentation*, which provides additional technical information about tolerance interdependencies and interchange verification testing, and also presents a conceptual overview of the design.
- The *trademark style guide*, which describes the use of the Ultrium trademarks and logos (Figure 1-2 on page 5).

Figure 1-2 LTO trademarks

1.1.3 Compliance verification

The technical strategy for accomplishing format compliance verification among the licensees has been defined, and an independent Compliance Verification Entity (CVE) has been selected. In an effort to promote interchangeability of tape cartridges, the TPCs are enlisting the services of a third-party verification test company to perform specification compliance verification testing. These tests will be required annually for all companies that use the logo.

The objective of the compliance testing is to test only the ability to produce and/or read and write Ultrium cartridges that meet the format specifications. It is not an objective of this format compliance testing to evaluate Ultrium drive quality, MTBF, physical form factor, or other parameters not directly related to the LTO program formats and interchangeability. LTO program licensees have wide latitude to establish their own mechanical, electrical, and logic designs to meet the format specifications. These factors will not be tested as part of the compliance verification process.

For more details about the packages, documentation, or licensing, refer to the LTO Web site:

`http://www.lto-technology.com`

1.2 LTO standards

LTO Technology was originally developed for two open tape format specifications: Accelis and Ultrium. The Accelis format (fast-access) is not being developed as the Ultrium format provides adequate fast-access performance.

1.2.1 Ultrium tape formats

Figure 1-3 on page 6 shows the IBM Ultrium cartridges, which can be distinguished by color: The first generation IBM cartridge is black, and the second generation (Ultrium 2) cartridge is purple.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1263
3698
Doc.

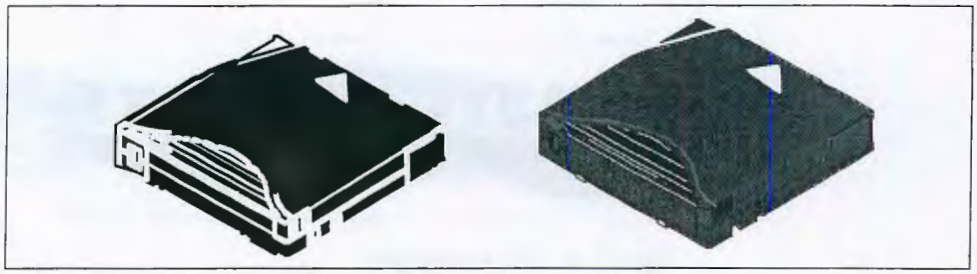


Figure 1-3 IBM LTO Ultrium 1 and Ultrium 2 tape cartridges

The Ultrium tape format specification is the implementation of LTO optimized for high capacity and performance with outstanding reliability, in either a stand-alone or an automated environment. The Ultrium cartridge uses a larger single-reel design (Figure 1-3) and 1/2-inch tape to provide ultra-high storage capacity. The tape is extracted from the cartridge by the tape drive through a leader pin, and wound onto a take-up reel contained within the drive itself. This design is focused on customer requirements for very high capacity and performance, and is ideally suited for backup, restore, and archive applications. Ultrium drive technology is intended to meet the needs of the enterprise on a roadmap, or migration path, that extends well into the future. The Ultrium tape format establishes a new benchmark for large volume backup and archive.

1.2.2 LTO core technology

Multi-channel linear serpentine recording is at the core of the LTO formats. It enables an optimum balance of reliability and data integrity, performance, and high capacity. In the LTO recording format, data is written in tracks that run down the length of the tape.

The Ultrium format records either 384 tracks (Ultrium 1) or 512 (Ultrium 2) across the half-inch of tape width. This linear recording format has a *serpentine* characteristic. The drive mechanism will make multiple passes from the beginning of the tape to the end of the tape and back in order to read or write the full capacity of the cartridge. In the Ultrium 1 format, the 384 tracks are split into four bands of 96 tracks each. In Ultrium 2 format, the 512 tracks are split into four bands of 128 tracks each. Data is written to the innermost bands first, to provide protection to the data recorded earliest in the process, by writing it in the center, the most physically stable area on the tape. Data is also verified as it is written. On pass one of a round trip down the length of the tape and back, eight tracks are read, or written, concurrently. At the end of the tape, pass two of the round trip starts. The read/write heads are indexed and positioned over eight new tracks, and the tape reverses direction back toward the beginning of the tape to

10.739

complete the round trip. For the next round trip, the heads are again indexed to a new position over a new group of eight tracks.

Because track densities are high, and because the tape is subject to some lateral movement as it is moved, it is critical for performance and data integrity that the read/write heads are always positioned precisely over the correct tracks. This is accomplished through a technique called timing based servo. This technique makes it possible to use high track densities, now and in the future, without changing the format of the media, and it provides the ability to read data, even with media imperfections.

In the LTO system, electronic signals are generated through the real-time reading of servo data bands that are prerecorded on the LTO tape. These signals enable the servo system to dynamically control the positioning of the read/write heads across the width of the tape. Similar magnetically based, track-following servo systems are proven in tens of thousands of tape drives in use today such as the IBM Magstar® High Performance Tape Drive.

The LTO formats also utilize advanced error correction codes for data integrity. These systems are designed to automatically correct most cross-track errors and provide data correction even if a full track is lost. Data is further protected by demarcation of bad areas of the tape (for example, where servo signals are unreliable) and through dynamic rewriting of bad blocks. Cartridge memory is embedded in the LTO cartridges. A non-contacting radio frequency module, with non-volatile memory capacity of 4096 bytes, provides for storage and retrieval of cartridge, data positioning, and user-specified information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1264
3698
Doc.

10.738
3

2

LTO technology

This chapter covers the LTO format specifications in general terms, including first and second generation Ultrium. The information referring to the data cartridge, the format in which data is written, elements of the drive specification relating to that format, and the compression algorithm description, are all part of the documented LTO specification. This kind of information will be applicable to all LTO manufacturers' product offerings in order to ensure cartridge interchangeability.

The information relating to the LTO Ultrium drive given in this chapter relates to the IBM LTO Ultrium drive, and may not be the same as those from other manufacturers in regard to such features as data rate and reliability.

This chapter also gives an overview of the IBM product offerings, which are covered in detail in later chapters.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1265
3698
Doc.

2.1 Interleaved recording

The drive uses an interleaved, serpentine, longitudinal recording format. The first set of eight data tracks is written from near the physical beginning of the tape to near the physical end of the tape. The head then repositions to the next set of tracks for the return. This process continues until all tracks are written and the tape is full.

The format of the recording of the data and servo tracks is defined as part of the LTO specification in order to meet the requirement for interchange between different manufacturers implementations.

2.1.1 Servo tracks

Servo tracks (also called bands) enable accurate positioning of the tape drive head over the data track, ensuring that the head does not stray onto an adjacent track. They are necessary to support high-data densities on the tape where the tracks are very close together. The servo bands are written at time of cartridge manufacture, before the cartridge is usable for data storage and retrieval.

Servo tracks are like lane markings on a multi-lane highway. Imagine how difficult it would be to drive on a highway without any lane markings. Lane markings help by positioning you on the lane, just as servo tracks support the drive recording head to position on the data tracks.

10.736

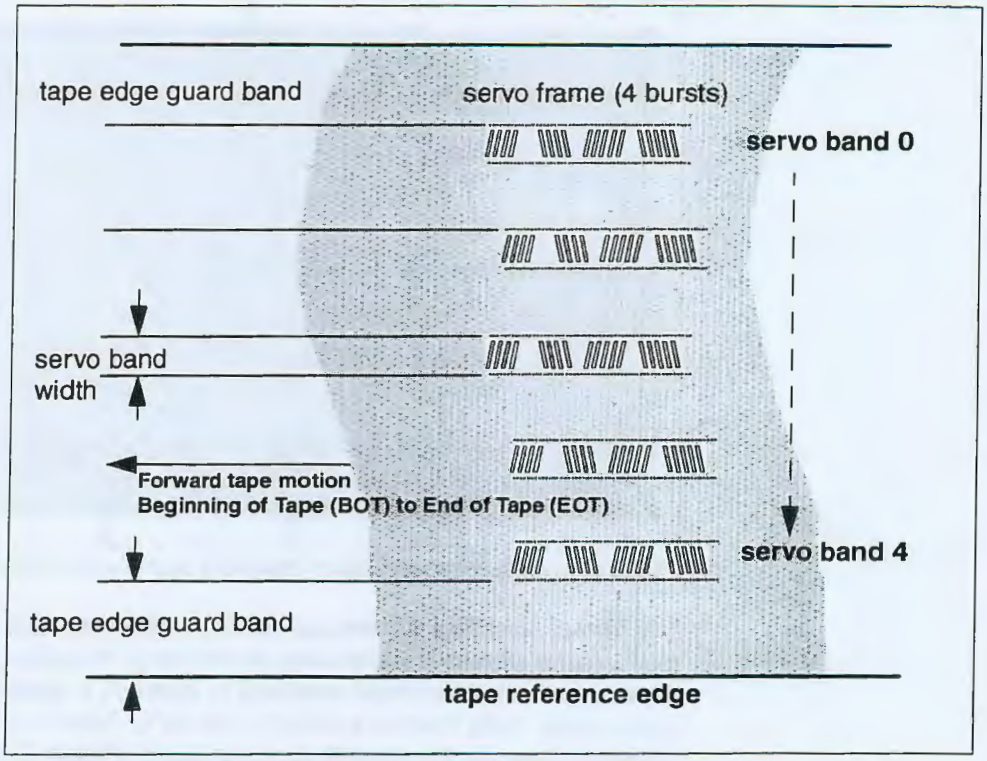


Figure 2-1 Servo band position and nomenclature

As shown in Figure 2-1, five servo bands, numbered 0 through 4, make up the servo tracking mechanism on the LTO Ultrium tape. They are each located at specific distances from the tape reference edge[1]. Within the servo bands are servo stripes, groups of which make up servo bursts. Four servo bursts make up a servo frame; the first two bursts (as written in the forward tape-motion direction) contain five servo stripes, and the second two bursts contain four servo stripes.

Track following

Each pair of servo bursts is at an angle to each other, and the servo heads move such that they keep a constant value for the distance between the bursts. In this way the servo is able to follow a straight line within the servo band; any small deviation away from the correct path causes a variation (plus or minus) in the gap between the bursts (see Figure 2-2 on page 12). Provided that the servo head element follows a straight line along the servo band, then the distance "x" shown in the figure remains constant. Two servo bands are used simultaneously to provide two sources of servo information for increased accuracy.

[1] The reference edge of the tape is the bottom edge when viewing the recording side of the tape with the hub of the tape to the observer's right, as shown in Figure 2-1.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 1266
3698
Doc.

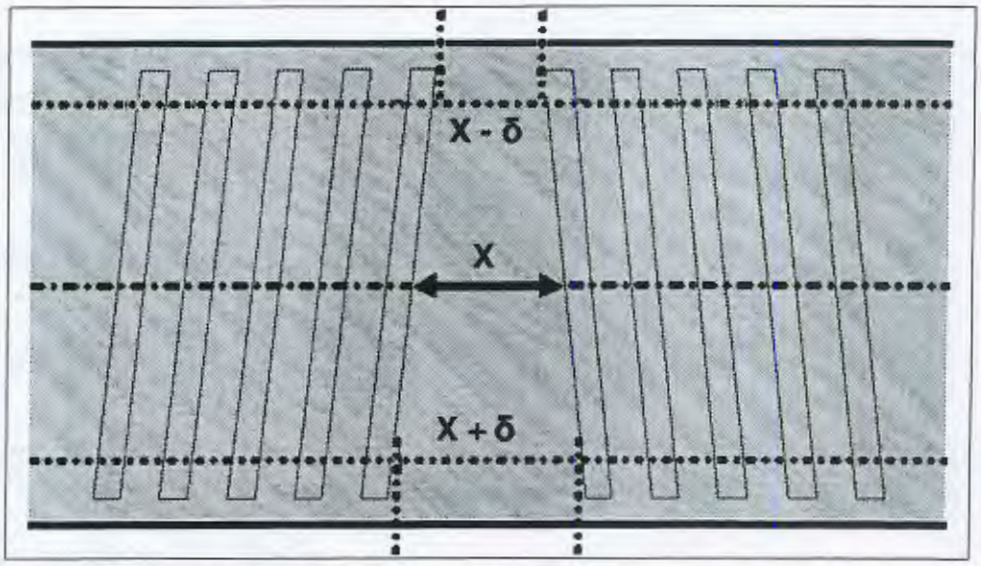


Figure 2-2 Magnified servo band showing a pair of servo bursts

The format specifies six nominal servo positions for Ultrium 1 and eight servo positions for Ultrium 2 within each servo band. In addition, the servo head is made up of two servo head elements to address a single servo band. This means that, using the two elements, the servo head is able to reposition within the servo band for the six (Ultrium 1) or eight (Ultrium 2) forward and reverse data wraps within each data band (Figure 2-5 on page 15). The distance between each servo position corresponds to the distance apart that the data tracks are written. For further information about the drive head and elements, see 2.4.1, "Drive head" on page 29 and Figure 2-15 on page 29.

This technology can be very finely tuned and is capable of supporting very high track densities using the same servo tracks because the currently used and defined six/eight nominal positions are basically definitions of six/eight different "x distances" between servo bursts (see Figure 2-2) and not a fixed servo track. By defining additional "x distance" positions, it is possible to increase the number of tracks on an LTO Ultrium while still using the same technology. With this technology, LTO is also able to satisfy the compatibility aspects as described in 1.1, "The LTO organization" on page 2. The Ultrium 2 drives have to use the six defined "x distances" on the Server tracks to read and write in Ultrium 1 Format.

Longitudinal positioning

The LTO servo band is designed not only for track following but also for recording the longitudinal position (LPOS). The absolute location down the length of the tape and the manufacturer data are recorded in LPOS "words," approximately

every quarter-inch (.7 cm) along the tape. The LPOS word consists of symbols constructed from bit sequences (ones and zeros); these bits are encoded within the servo frames.

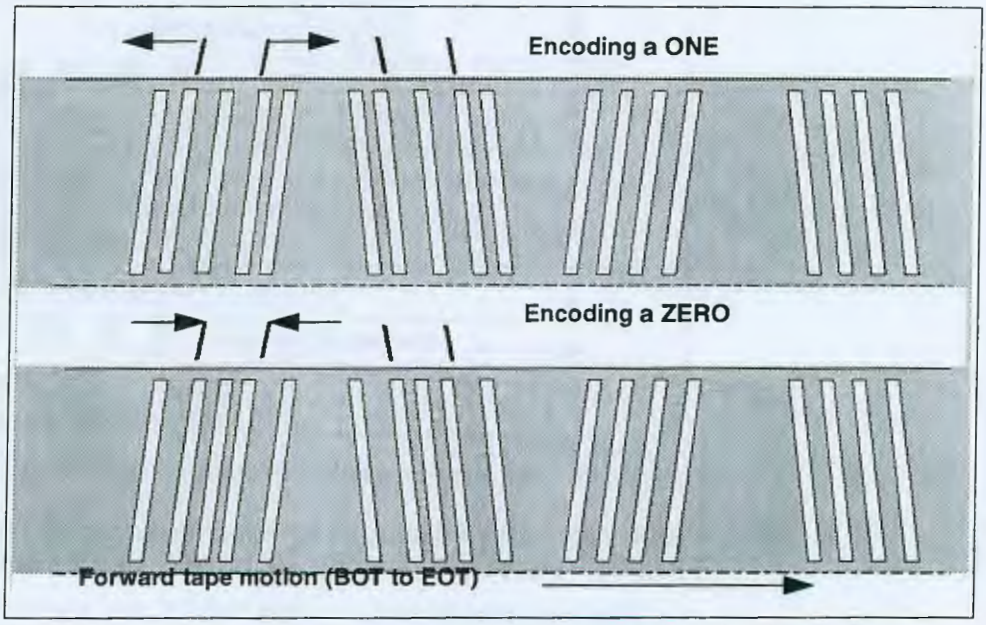


Figure 2-3 Encoding bits using the servo stripes within the servo bursts

Each servo frame encodes one bit using the first pair of servo bursts. When servo stripes 2 and 3 (out of the five) are shifted inward (see Figure 2-3), this encodes a zero; when servo stripes 2 and 3 are shifted outward, this encodes a one. The LPOS word contains 36 bits and thus has a length of 36 servo frames.

Each of the 5 servo bands on the tape may be uniquely identified by the relative positions of the frames down the tape, in adjacent servo bands. The offset of the frames between servo band n and servo band $n+1$ are specific to each servo band (0 and 1, 1 and 2, 2 and 3, or 3 and 4). Thus the drive can move the head directly from the physical beginning of the tape to a specific logical position for reading or writing.

2.1.2 Data tracks

The area between adjacent servo bands is a data band. There are four data bands numbered 2, 0, 1, and 3, where data band number 2 is nearest the reference edge of the tape and data band 3 is farthest away, as in Figure 2-4 on page 14. The data bands are written in sequence beginning with 0 (in the center of the tape) and ending with 3.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1267
Fls Nº
3698
Doc.

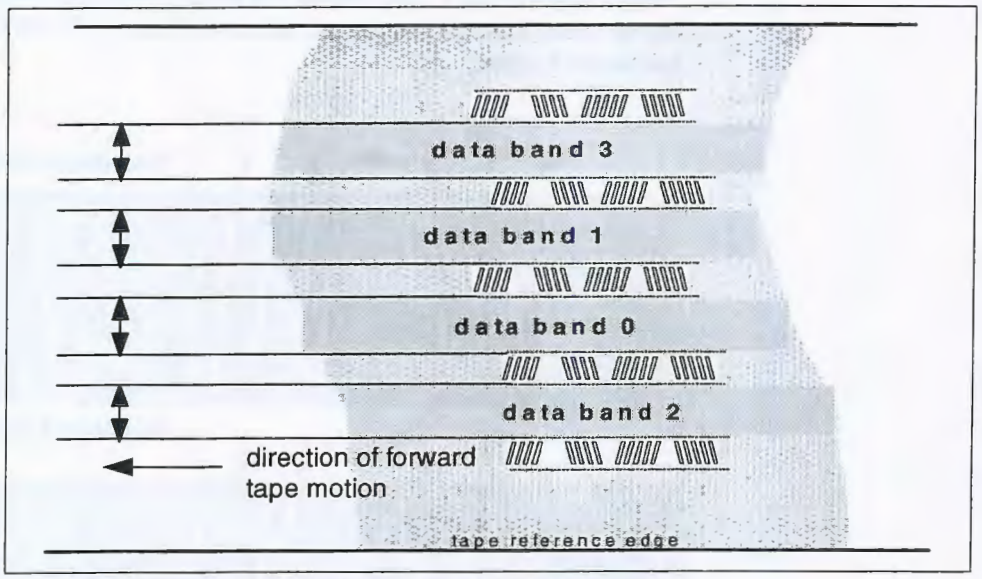


Figure 2-4 Four data bands written between the servo tracks

Each data band consists of numbers of tracks that are recorded eight tracks at a time from one end of the tape to the other in the following way:

- The head is positioned over data band 0, and the first set of eight tracks is written from the physical beginning of the tape to the physical end.
- The head physically repositions (using a different servo position within the same servo bands) and switches electronically[2] to a second set of eight write elements in order to write eight tracks in the reverse direction back to the physical beginning of the tape.
- The head physically repositions again, and, switching back to the first set of write elements, writes another set of eight tracks to the physical end of the tape.
- The head continues to switch and index in this manner until all 96 tracks are written and the head is back at the physical beginning of the tape.
- The head moves to data band 1 to continue writing the data.

For Ultrium 1, 96 data tracks coexist in one data band. For Ultrium 2, there are 128 data tracks in one data band.

A group of tracks recorded concurrently in the physical forward or the physical backward direction is called a *wrap*. Wraps recorded while the tape is moving from BOT to EOT are forward wraps; wraps recorded while the tape is moving

[2] See 2.4.1, "Drive head" on page 29 for more information about electronic head switching.

from EOT to BOT are reverse wraps. The wraps are recorded in a serpentine fashion, as described: a forward wrap, then a reverse wrap. They are numbered sequentially in the order that they are processed, starting with wrap 0. Thus, for Ultrium 1 six forward wraps and six reverse wraps make up a data band. For Ultrium 2, eight forward and eight reverse wraps make up a data band. The individual tracks within a wrap are interleaved with tracks from other wraps; in other words, adjacent tracks are not part of the same wrap. (See Figure 2-5.)

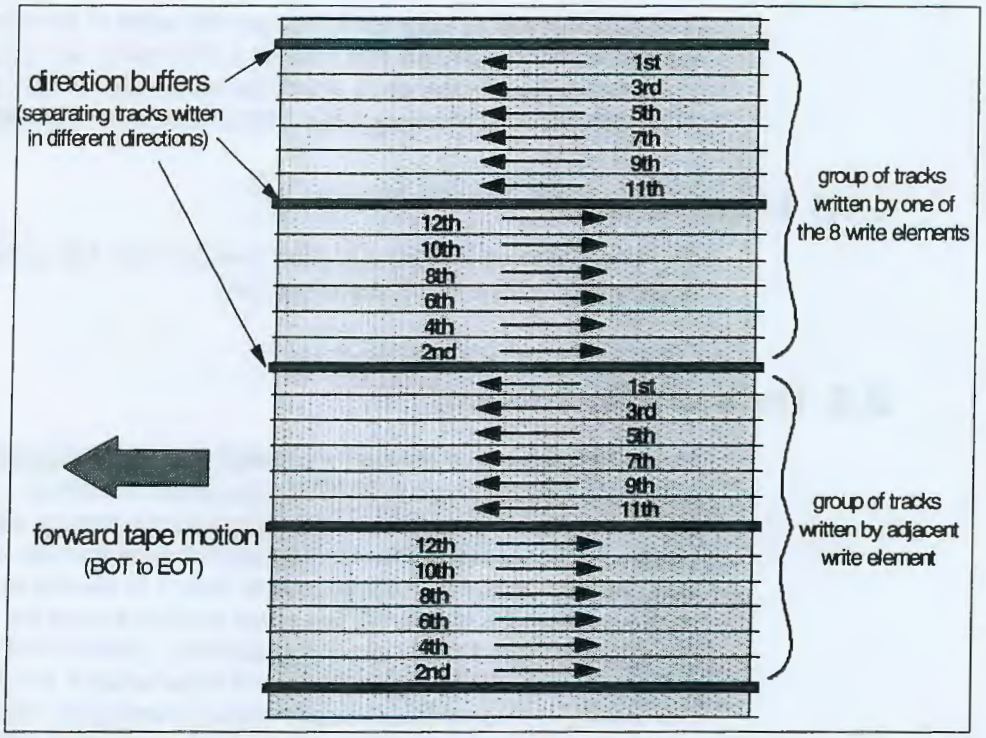


Figure 2-5 Portion of data band showing Ultrium 1 track-writing sequence

This figure expands on Figure 2-4 on page 14 to illustrate the sequence in which the tracks are written. One data band is magnified[3] to show an area written by two adjacent write head elements (from the total of eight); this is one quarter of the width of the data band. You can see that the tracks are written in an inward spiral (serpentine) manner; the first and second tracks are farthest away from one another while the 11th and 12th tracks are adjacent to one another.

[3] Refer to 2.4.1, "Drive head" on page 29, and Figure 2-15 on page 29, to see the structure of the eight-element head.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1268
Doc. 3698

The space between tracks written in opposing directions is called a direction buffer. This space is designed to minimize magnetic interference between tracks written in opposite directions (cross-track interference).

Read/verify elements are built into the tape head in the drive. The data is written by the write elements and then immediately passes the read/verify elements and is checked for errors. If any errors are found, the block of data is rewritten farther down the tape.

The total number of data tracks across the width of the tape is 384 for Ultrium 1, numbered 0 through 383. For Ultrium 2, 512 tracks are used. Track numbering is unrelated to the sequence in which the tracks are written: data track 383/512 is the closest to the reference edge of the tape, and data track 0 is farthest away.

2.1.3 Linear density

The linear density for LTO 1 is 4880 bits per mm. The linear density was improved for LTO 2 to 7398 bits per mm.

2.2 Data compression

The LTO Consortium created a superior data compression technique know as LTO Data Compression (LTO-DC). Though an excellent data compression algorithm, ALDC (adaptive lossless data compression), already exists, ALDC function is not optimized for incompressible data such as encrypted or previously compressed data. For incompressible data, it is usually best not to apply any data compression algorithm, but rather to simply pass the input data out to the compressed data stream directly (pass-thru). Given the variations in data, there are times when ALDC is desirable and times when a simple pass-thru is better. For instance, if using ALDC-based data compression, it would be best if all segments of incompressible data were to be recorded without expansion by using a pass-thru technique instead. Figure 2-6 is a block diagram illustration of the LTO-DC data compression technique using the two schemes.

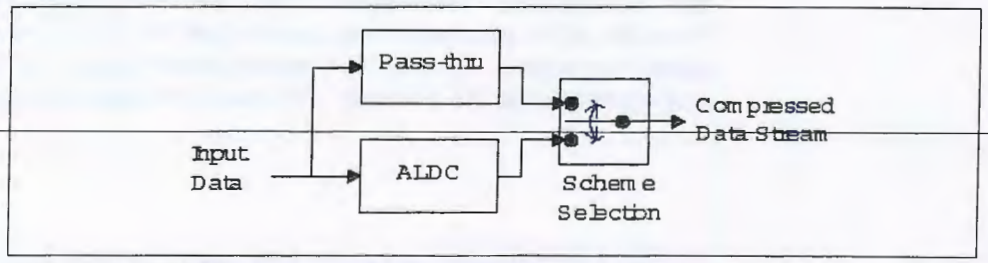


Figure 2-6 LTO-DC block diagram

10.730

Note that no standardization of when to scheme swap when compressing data was specified by LTO-DC. LTO-DC was approved by ECMA as SLDC [streaming lossless data compression] standard, as explained at:

`http://www.ecma-international.org/publications/standards/ECMA-321.htm`

Because no standardization is specified, all vendor implementations may do scheme swapping differently. What is specified and tested is that the resultant compressed data stream is decompressible by the defined set of LTO-DC rules. This enables interchange between drives from the three companies. Each vendor's Ultrium drive has been shown to be able to read and decompress the LTO-DC streams of the others.

Embedded codewords

LTO-DC uses embedded codewords to enable swapping between the two schemes. ALDC is referred to as Scheme 1, and pass-thru is referred to as Scheme 2. Both methods are used. However, only one is used to output any given data byte, though different bytes in a record might be output in different schemes. Thus, if a given record begins with compressible data it can be output in Scheme 1, and if the nature of the data changes inside of the record and it becomes incompressible (as embedded control data or an array of incompressible data), a scheme swap can be performed to allow outputting the incompressible data in Scheme 2. Similarly a scheme swap can be performed to revert to Scheme 1 if the data becomes compressible again. A scheme swap is denoted in the compressed data stream via one of four embedded codewords. As an example, one 13-bit codeword basically means all following data is to be decompressed as Scheme 1 until another scheme swapping codeword is encountered. Embedded codewords are also used to delineate record boundaries and filemarks. Having record boundaries demarked within the output compressed data stream, rather than by pointers maintained in a separate directory table, has a number of advantages. First, from a storage point of view, it is more efficient as it enables greater capacity. Second, the insertion of these codewords enables higher-speed data streaming because they can be managed by the compression engine without microprocessor involvement. Both of these features are especially useful for small records. Typically, backup applications will send 512-byte, 4-KB, 32-KB, or 256-KB records to a backup tape drive. For small records such as 512 bytes, the improved format efficiency of the embedded control is substantial. By reducing required microprocessor involvement it allows superior transfer rates to the drives. This is why LTO tape drives offer high capacity tape backup, as well as drive transfer rates far better than other midrange backup tape drives—and are superior even to some costly, high-end tape drives.

The ability to swap between ALDC and a pass-thru mode gives a tape drive the power to automatically adapt to the incoming data stream.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1269
3698
Doc.

2.3 Tape cartridge

The Ultrium cartridge is a single-reel cartridge. This means the whole tape is wrapped around a single reel when the cartridge is not loaded in a drive. During the loading process, the threader of the drive catches the leader pin of the tape and threads it through the drive and the machine reel. During the read/write process the tape is stored on the machine reel and the cartridge.

Two views of the tape cartridge are shown in Figure 2-7 and Figure 2-8 on page 19.

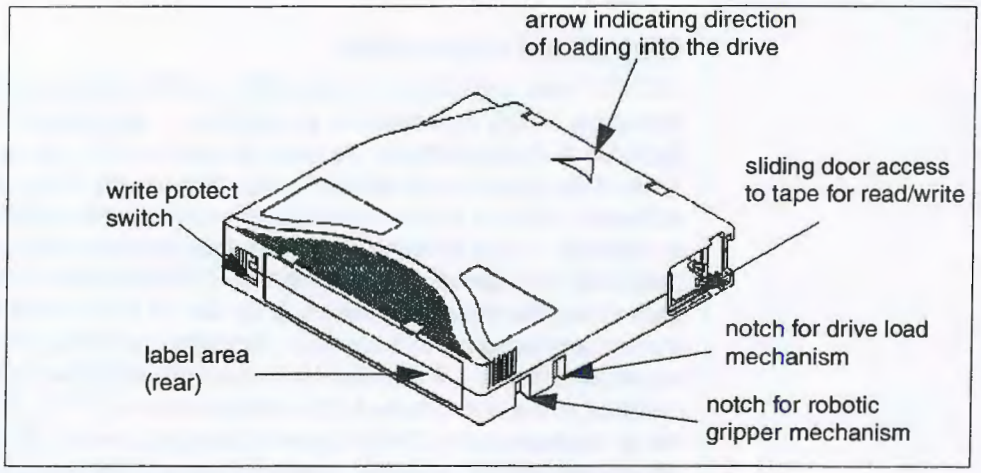


Figure 2-7 Ultrium cartridge view from top and rear

The cartridge is approximately 10.2 cm long, 10.5 cm wide, and 2.2 cm high (approximately 4 x 4.16 x 0.87 inches). The cartridge contains 1/2-in (12.6 mm), metal-particle tape with a highly dense recording area. The Ultrium 1 spec describes four types of cartridges, each with a different tape length and, therefore, capacity. At this time, only one cartridge type is generally available, with a tape length of 610 m (2000 feet) providing 100 GB of native data and 200 GB of compressed data (assuming 2:1 compression). There is only one standard Ultrium 2 cartridge type and hence only one tape length of 610m (2000 feet). The native capacity of the Ultrium 2 cartridge is 200 GB (400 GB compressed assuming 2:1 compression).

Figure 2-8 on page 19 shows some of the components of the cartridge.

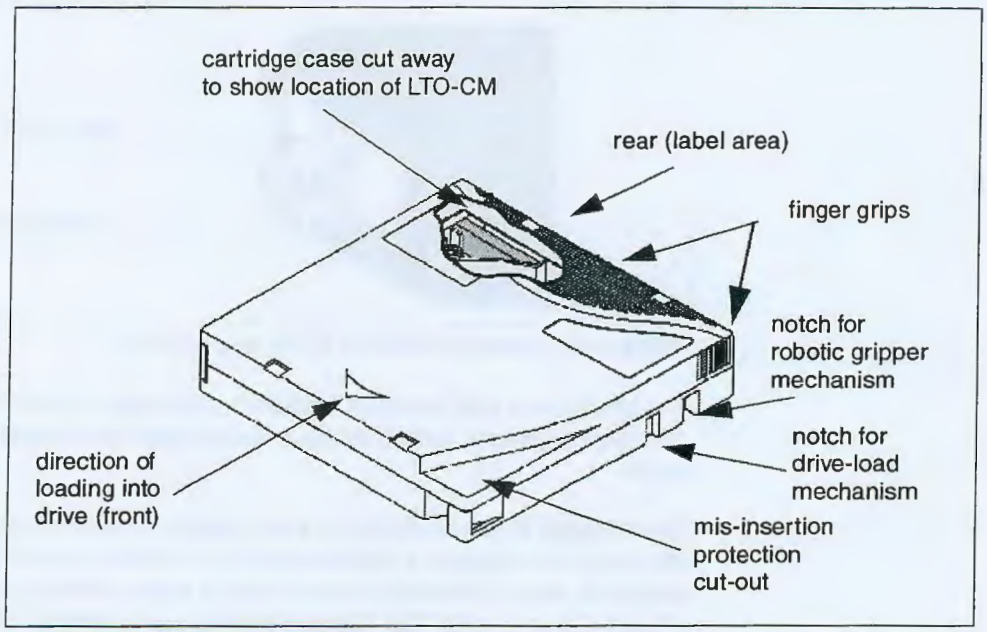


Figure 2-8 Ultrium cartridge view from top and front

The labelled parts are:

- Grips: Molded areas on the cartridge casing designed as finger grips for manual loading.
- Label area: Located at the designated area at the rear of the cartridge where the adhesive bar code label is applied.
- Sliding door: Cartridge door (shown in Figure 2-7 on page 18) that protects the tape from contamination whenever the cartridge is out of the drive. Behind the door, the tape is threaded onto a leader pin (shown in detail in Figure 2-9 on page 20), which is used to pull the tape from the cartridge for use. A locking mechanism prevents the media from unwinding when the cartridge is not located in the drive.
- Notches: Two sets of moulded notches in the cartridge casing located on the sides near the rear. The first pair enables the robotic gripper to pull the cartridge out of the drive mouth once the cartridge has been unloaded; the second pair enables the drive to grip the cartridge and pull it into the loading position inside the drive.
- Mis-insertion protection: A cut-out in the front side of the cartridge casing that prevents the cartridge from being inserted into the drive in the wrong orientation. This feature prevents the use of unsuitable cartridges of similar, but not identical, construction.

RQS nº 03/2005 - CN
CPMI
Fls. Nº
Doc 3698

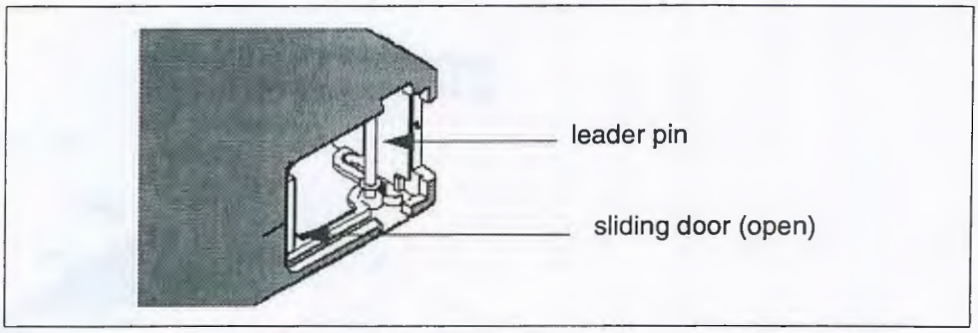


Figure 2-9 Leader pin attached to the tape medium

The shell of an IBM branded Ultrium 1 cartridge is black and of an Ultrium 2 cartridge is purple, providing easy visual distinction between the two media types.

Even though the servo tracks are the same on Ultrium 1 and Ultrium 2 cartridges, Ultrium 2 cartridges are required with an Ultrium 2 drive to achieve Ultrium 2 capability. More information about media compatibility between Ultrium 1 and Ultrium 2 is in 2.4.7, "IBM Ultrium 1 and 2 compatibility" on page 39.

2.3.1 Metal particle medium

The metal particle tape medium consists of a transparent polyethylene base material with two coatings. On one side, the base has two fine coats of a strong yet flexible ferromagnetic material, dispersed in a suitable binder; this is the surface on which the data is written. The back surface is coated with a non-ferromagnetic conductive coating.

Metal particle media have high coercivity, which is a measure of their ability to retain their magnetic properties once the data is written to the tape; this is one of the factors in enabling a potentially longer shelf life than other media.

2.3.2 Cartridge memory (LTO-CM)

Information about the cartridge and the tape is written to the LTO-CM, which is a serial EEPROM with both read-only and rewriteable areas. It is housed inside the cartridge casing at the left rear (label side) corner as illustrated in Figure 2-8 on page 19, which shows the interior of the cartridge casing.

The LTO-CM has a capacity of 4096 bytes. It is used to hold information about that specific cartridge, the media in that cartridge, and the data on the media. A copy of this information is also kept in the first data set within the user data area, and is given the data set number zero.

Communication between the drive and the LTO-CM uses a contactless low-level radio frequency (RF) field generated (in the IBM implementation) by the drive. The LTO-CM is non-volatile storage updated using the RF field; it requires no additional power source. This type of technology has an expected shelf life of more than 30 years.

There are a number of distinct data fields within the LTO-CM, shown in Table 2-1. The fields align to 32-byte boundaries, as this is the defined block access size.

Table 2-1 Data fields stored in the LTO-CM

LTO-CM information	Read/write
LTO-CM manufacturer's data	Read-only
Tape label[a]	
Media manufacturer information	
Initialization data[b]	Restricted write capability
Cartridge status and tape alert flags	Read or write
Usage information	
Tape write pass	
Tape directory	
End-of-data information	
Mechanism related	
Application specific data[c]	
Vendor unique data	

a. This field contains information about the tape, including a 10-byte field with the tape serial number; it is a read-only area and does not contain the volume label, which could be changed if the tape is reinitialized.
b. This is a restricted-write field that is updated with changes when the tape is reinitialized.
c. This is a field for application data (such as the volume label) to be stored in the CM. However, currently there is no SCSI function available to support writing to that area.

Although transparent to the user, keeping this kind of information enhances the efficiency of the drive and cartridge. Data and block locations are stored in memory; for example, the end-of-data location is stored, so that when the tape is next loaded, the drive can use the fast locate function to move directly to the recording area and begin recording. Storing data about the age of the cartridge, how many times it has been loaded, and how many errors it has accumulated

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1271
Doc 3698

aids in determining the reliability of the cartridge. It is of particular value if this data is stored with the cartridge itself, so that whenever it is mounted on any host system, the history is accessible.

This is not the first tape product where information has been kept on the cartridge; however, previously it has been written onto the tape medium itself in a non-user-accessible portion of the tape before the beginning-of-tape (BOT) marker, for example, as in the IBM 3590 tape drive.

2.3.3 Barcode label

Each data and cleaning cartridge processed by an Ultrium tape library should bear a barcode label. (This is mandatory for libraries that have an installed barcode reader such as the IBM 3584.)

The label, as shown in Figure 2-10, contains a human-readable volume serial number or volume label, and a machine-readable barcode.

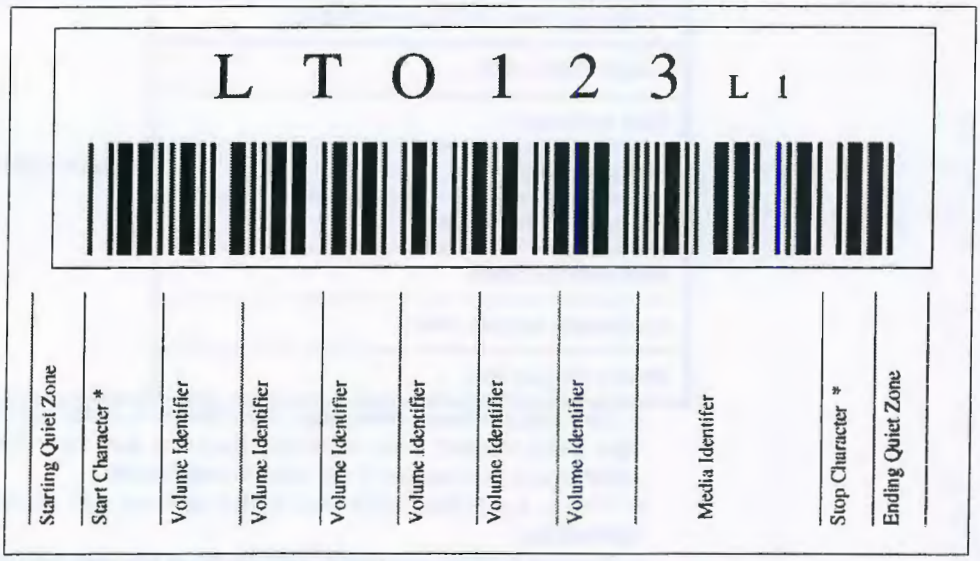


Figure 2-10 Barcode label example

The bar code format is:

- Quiet zones (at each end of the bar code)
- A start character (indicating the beginning of the label)
- A six-character volume label

- A two-character cartridge media-type identifier (L1 or L2), which identifies the cartridge as an LTO cartridge ('L') and indicates that the cartridge is the first ('1') or second generation ('2')
- A stop character (indicating the end of the label)

When read by the library's barcode reader, the barcode identifies the cartridge's volume label to the tape library. The barcode volume label also indicates to the library whether the cartridge is a data, cleaning, or diagnostic cartridge.

Tape cartridges are often supplied with the labels already attached, or you can attach a label yourself. Operators must handle the cartridges and barcode labels in accordance with the instructions in the operator guides supplied with the products. You must ensure that labels are removed cleanly, reapplied carefully, in good condition, and not obscured or damaged. The Ultrium cartridge features a recessed area for the label (see Figure 2-7 on page 18). The label must be applied only in the recessed label area; if it extends outside of the area it can cause loading problems in the drive.

2.3.4 Volume label format

The LTO cartridge label uses the USS-39 barcode symbols. A description and definition is available from the Automatic Identification Manufacturers (AIM) specification document *Uniform Symbol Specification (USS-39)* and *ANSI MH10.8M-1993 ANSI Bar code Specification.*

A cartridge's volume label consists of exactly 6 characters, starting from the left. Except for cleaning and diagnostic cartridges, these 6 characters are limited to the following ASCII characters:

- Upper-case A-Z (ASCII character code: 41h-5Ah)
- 0-9 (ASCII character code: 30h-39h)

The volume label must consist of exactly six, all upper-case alphabetical, all numeric, or alphanumeric characters, such as ABCGVE, 123621, or F8H5N9. It cannot consist of fewer than six characters.

A volume label format of CLN*Unn* represent a universal cleaning cartridge. A volume label of the form CLN*vnn* is used for a unique cleaning cartridge, where *v* is an alphanumeric identifier that represents the vendor of a drive-unique cleaning cartridge. (An IBM-unique cleaner cartridge uses the label format CLNInn.) This identifier is logged in the vendor information pages in the Ultrium tape drive.

A volume label of the form DG(space)*vnn* is used for diagnostic and service cartridges. The drive uses the '*v* to determine if the drive-unique diagnostic

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1272
Doc. 3698

cartridge is loaded. The '*nn*' represents a specific cartridge and is logged in the vendor information pages in the Ultrium tape drive.

The internal and external labels on a cartridge need not match; this means that the volume label on the bar code label need not match the volume label recorded on the tape in the tape label area when it is initialized. However, it is generally preferable for them to match to avoid confusion.

You will find more detailed information in the LTO Label specification at:

`http://www.storage.ibm.com/media/`

2.3.5 Write protect switch

The write protect switch is located at the front of the cartridge to the left of the bar code label (see Figure 2-7 on page 18). The position of the write-protect switch on the tape cartridge determines whether you can write to the tape; you cannot write to the tape when the switch is pushed to the right. When the write protect switch is set to inhibit writing, a visual lock mark such as a padlock will be visible.

In most cases, backup and recovery host application software is used to achieve the most benefit from using an LTO system. It is better to rely on the host application software to write-protect your cartridges rather than manually setting the write protect switch. This allows the host software to identify a cartridge that no longer contains current data and is eligible to become a scratch cartridge. If the switch is set and the host application sets the cartridge to scratch status, the tape drive will not be able to write new data to the tape.

2.3.6 Cleaning the cartridge

Cartridges that are physically dirty on the outside of the casing can reduce the reliability of an Ultrium tape library as well as cause the loss of recorded data. If dirt appears on the cartridge, you can wipe the outside surfaces with a lint-free cloth, which may be lightly moistened with the manufacturer's recommended tape unit cleaner or equivalent.

When cleaning a tape cartridge, do not allow anything wet (including the cleaning fluid) to contact the tape inside the casing. Make sure that all cartridge surfaces are dry before the cartridge is inserted in a drive.

2.3.7 Cartridge life

The magnetic tape inside the cartridge is made of highly durable materials. However, the tape wears after repeated cycles. Eventually, such wear can cause an increase in tape errors, records of which are stored in the LTO-CM. This

means that cartridge performance can be tracked and monitored, enabling predictive failure analysis and enhancing data integrity. This tracking is done automatically, and the drive issues a message when errors on the tape exceed a certain threshold.

The IBM Ultrium Data Cartridge has a usable life of 5000 load and unload cycles in a typical office computer environment.

The data recorded on the cartridge has an archive storage life of 30 years minimum with less than 5% loss in demagnetization, when the cartridge is stored at 16° C to 25° C, 20% to 50% non-condensing humidity, and wet bulb temperature of 26° C maximum.

2.3.8 Cleaning cartridge

To support customer and application requirements and expectations for cleaning, each LTO drive vendor used to provide its own cleaning cartridge specifically for its Ultrium drives. To avoid potential interoperability problems, the LTO consortium decided to introduce a universal cleaning cartridge. IBM offers only the universal cleaning cartridge.

The IBM Ultrium LTO tape drive was intentionally designed to not require cleaning but rather to be self-monitoring and self-cleaning. Therefore the IBM recommendation is not to manually clean the tape drive regularly, but rather to use the automatic cleaning function provided with the library or by your application. Each drive determines when it needs to be cleaned and alerts the library or your application.

The cleaner cartridge can be used a maximum of 50 times to prevent recontamination of drive surfaces.

2.3.9 Cartridge handling

Tape cartridges are tough packages made of inexpensive materials capable of storing tremendous amounts of data and approaching data densities of hard disks. They can survive for years in library environments where they are being gripped and poked, loaded and unloaded. But we recommend treating tape cartridges in a similar fashion to hard disk drives. Here are some suggestions to protect your data on tape cartridges.

Ensure that proper procedures are in place to cover media handling, and make sure that anyone who handles cartridges has been trained in those procedures.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1273
Doc: 3698

Media shipping and handling: procedures

Ship cartridges in their original packaging, or preferably, ship/store in jewel cases. Use only recommended shipping cases that securely hold the cartridges in their jewel cases for transportation. Turtle Cases from Perm-A-Store at www.turtlecase.com, shown in Figure 2-11, have been tested and found to be satisfactory.

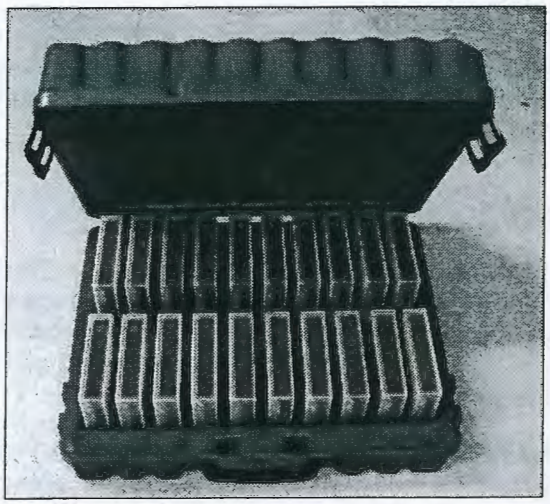


Figure 2-11 Turtle case

Never ship a cartridge in a commercial shipping envelope without boxing or packaging. If shipping in cardboard or similar boxes:

- Double-box the cartridges with padding between the boxes, as shown in Figure 2-12 on page 27.
- Pack snugly so cartridges do not rattle around.
- If possible, place cartridges in polyethylene plastic wrap or bags to help seal out dust, moisture, and other contaminants.

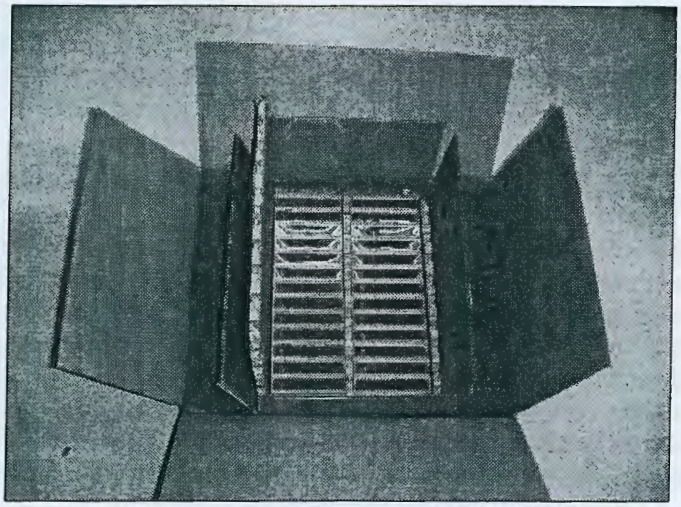


Figure 2-12 Double box

Media shipping and handling: inspecting

If you receive media, inspect it before use:

- Inspect packaging for evidence of potential rough handling.
- Inspect cartridge for damage before using/storing.
- Check leader pin for correct seating.
- When there is evidence of poor handling or shipping, ensure the cartridge leader pin (Figure 2-13) is undamaged before inserting the cartridge in a drive or library, as a bad cartridge can damage a drive.

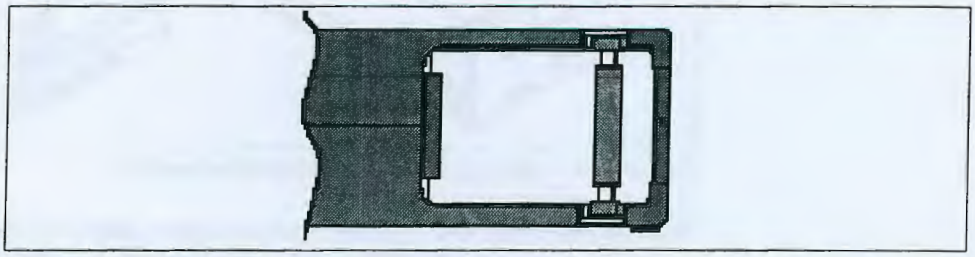


Figure 2-13 Correct leader pin placement

If the pin is loose or bent, then look for cartridge damage and use the IBM Leader Pin Re-Attachment Kit - Part Number 08L9129 to correctly seat the pin.

Summary

- Package appropriately for shipping.

RQS nº 03/2005 CN
CPMI CORREIOS
Nº 1274
Doc 3698

- Inspect for damage or rough handling and take appropriate action.
- Do not put damaged media in drives or libraries; use data recovery services.
- For specific media types, check your product's Planning and Operator Guide.
- With simple care and handling you can get the most out of your tape media.

2.4 IBM LTO Ultrium common subassembly

Some elements of the Ultrium drive design are covered by the LTO format specification, such as anything related to writing the specified data format that enables tape interchange. However, there is no strict LTO definition in terms of how the drive module is constructed, so in this area, manufacturer's drives may differ from each other in performance and specification, such as data rate or quality design points. This section therefore relates specifically to the IBM LTO implementation. However, we emphasize again that the IBM LTO Ultrium cartridges are compatible with those of all other licensed manufacturers.

The IBM LTO Ultrium common subassembly drive (Figure 2-14) is a high-performance, high-capacity tape drive. The drive records data using the specified linear serpentine recording format on 1/2-inch tape housed within the LTO Ultrium cartridge. The data tracks are located using preformatted servo tracks, as outlined in 2.1.1, "Servo tracks" on page 10.

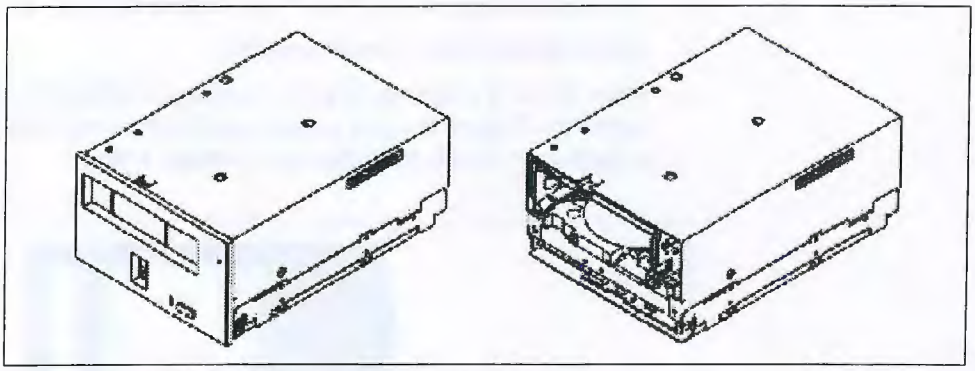


Figure 2-14 IBM LTO Ultrium common subassembly

The original basic unit was the first-generation IBM LTO series of products. The second-generation IBM LTO is a further development with a high amount of reuse, making the IBM Ultrium 2 drive very reliable. These units are a common subassembly and so do not have an IBM machine type. The subassembly is not available for end-user customers to purchase, but only as a part number used in the assembly of other IBM machine types. It does not have its own power supply but is powered by the library, frame, or casing into which it is integrated.

The IBM machine types that integrate the subassembly are described in 2.5, "The IBM LTO Ultrium family of tapes and libraries" on page 44, and in more detail in later chapters. The subassembly is sold on the OEM market to other LTO library manufacturers. The common subassembly is a single field replaceable unit (FRU): that is, if it fails the whole unit is replaced and no parts or subassemblies within the unit are replaced when the drive is maintained by a service representative.

2.4.1 Drive head

When the cartridge is inserted into the drive, a threading mechanism pulls the leader pin and attached tape (see Figure 2-9 on page 20) out of the cartridge, across the read/write head, and onto a non-removable take-up (machine) reel. The head can then read or write data from or to the tape.

The drive has a 2 x 8 element head, reading or writing data eight tracks at a time (see Figure 2-15). The head is sized to cover the width of a data recording band (approximately a quarter of the tape width; see Figure 2-4 on page 14). Unlike the IBM 3590, for example, it does not cover the whole width of the tape.

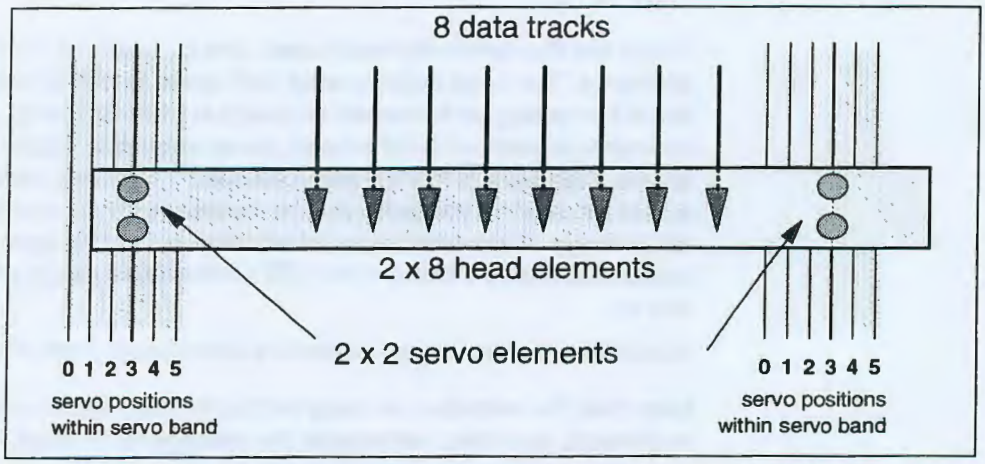


Figure 2-15 Eight-element head (one set of heads shown) and servo elements

The write elements are immediately followed by read/verify elements, so there are in fact two sets of eight head elements (eight write elements and eight read elements) to allow the tape to write in the forward and reverse directions down the length of the tape. The head switches electronically from one set to another as the tape changes direction, as in Figure 2-16 on page 30, which shows two enlarged pairs of head elements and the direction indicators. Two sets of heads (r-w and w-r) are required because the tape is written and read in both directions.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1275
3698
Doc:

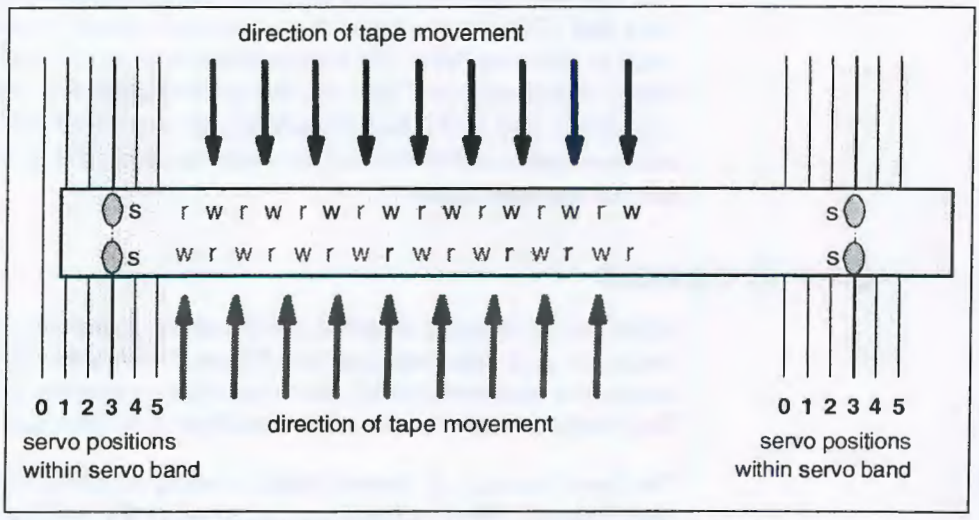


Figure 2-16 Allocation of read and write heads for forward and reverse wrap

The mechanism for writing data is explained in section 2.1.2, "Data tracks" on page 13.

There are four servo elements used, two for each set of eight read/write elements. The head actually uses both servo tracks at each edge of the data band it is writing for increased accuracy in track-following, so there are two servo elements at each end of the head. As an example, Figure 2-15 on page 29 shows a diagram of the top servo element 1 following servo position 3, which would be used for the sixth wrap (a reverse wrap) in a data band; the diagram is not to scale. If you need more information about this topic, an animated explanation can be found in the LTO Ultrium technology primers on the LTO Web site at:

`http://www.lto-technology.com/newsite/html/about_tech.html`

Note that the animation is designed to provide a basic understanding of LTO technology and does not provide the same level of detail outlined here.

2.4.2 Data compression

As describes in 2.2, "Data compression" on page 16, the implementation of the data compression may be different from vendor to vendor.

One implementation appears to only perform scheme swapping on a record basis. For example, if the compressed data stream output for a given record is larger for Scheme 1 than for Scheme 2, then the entire record is output in Scheme 2. The second implementation seems to react to data on an ongoing

basis so that if the drive perceives that the nature of the data in a record has changed from compressible to incompressible then a Scheme 2 swap is enabled and the incompressible data from there on is output in Scheme 2. This is not always advantageous because the incompressible data may again transition to compressible even before that scheme swap has occurred. Each scheme swap codeword output is 13 bits long. Therefore, to swap to a scheme and swap back costs 26 bits. The compression gain following the first scheme swap may benefit more than 26 bits over the previous scheme; if so, the swap was well-advised. If not, then the scheme swap actually increased the size of the output compressed data stream and reduced the compression rather than increase it. There is a chance of this occurring if data compressibility is inferred by having the data compression engine observe how data that has already been output from the compression engine was compressed—that is, only by viewing data in the past. The only way to adapt via scheme swapping within records, without being susceptible to inadvertent data expansion, is to use the IBM-patented scheme swapping technique. This method is preferred since it effectively looks at data ahead, rather than behind. In the IBM implementation, a scheme swap is not automatically generated unless there appears to be more compression gain within the look ahead buffer than it costs to scheme swap, and then swap back. This is advantageous as small bursts of compressible data within an otherwise incompressible file may not make it worthwhile to scheme swap. If a scheme swap is optimal, the IBM implementation puts the scheme swap out where the change in data compressibility occurs, giving maximum advantage. For more information, see:

`http://www.storage.ibm.com/hardsoft/tape/lto/prod_data/whitepaper_compression.pdf`

This paper shows how the IBM LTO-DC embodiment achieved superior data compression to another vendor's LTO drives by performing scheme swapping simultaneously with changes in the compressibility of the data, enabled by effectively looking 64 bytes ahead in the input data stream.

2.4.3 Interfaces

The IBM LTO Ultrium drive is available with a choice of interfaces, either SCSI LVD or HVD, or FC. When ordering an IBM product offering, you choose the drive interface. You cannot change the interface on the drive; if you want a different interface, you must replace the drive assembly.

Common interfaces for tape drives

Historically, SCSI connections were used for attachment of tape drives and libraries to open systems. Fibre Channel connections using SANs are becoming increasingly common.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1276
Doc. 3698

SCSI single ended

This was the most common form of SCSI signaling. Many removable drives, scanners, and almost all 50-pin SCSI devices fit into this category. Often you do not see "SE" or "single-ended" written on the documentation; if a device does not specifically say LVD, Ultra2 Wide, differential, or some similar definition, then it is probably single-ended. Typically, single-ended devices support a total bus length of 1.5 meters (5 ft) or less.

IBM high-performance SCSI tape drives (IBM 3590, IBM 3570, and LTO Ultrium drives) are all differential-attached drives, not single-ended.

SCSI differential (HVD)

HVD (often referred to as just "differential") uses differential signaling. The idea behind differential signals is that each bus signal is carried on a pair of wires. The first wire of the pair carries the same type of signal as single-ended SCSI. However, the second wire of the pair carries its logical inversion. The receiver of the signals takes the difference of the pair (hence the name), which makes it less susceptible to noise and capable of supporting greater cable lengths. HVD and single-ended SCSI are completely incompatible with each other.

In general, IBM HVD tape devices support an overall bus length of 25 m, using point-to-point or multi-drop interconnection (daisy-chaining). For each daisy-chain device you have to reduce the maximum cable length by 0.5 m.

SCSI differential (LVD)

This newer differential interface implementation, LVD uses less power than the HVD differential interface, and allows the higher speeds of Ultra-2 SCSI. LVD requires 3.3 V dc instead of 5 V dc for HVD.

LVD is sometimes referred to as Ultra-2 Wide SCSI, which is a general marketing term for 16-bit Fast-40 or 80 MB/s. Only LVD and HVD could potentially run in Ultra-2 Wide mode, and only LVSD in current commercially available products.

IBM LVD tape devices support a bus length of 25 m point-to-point, and 12 m using multi-drop interconnection (daisy-chaning). For each daisy-chain device you have to reduce the maximum cable length by 0.5 m.

The terms fast, wide, and ultra indicate characteristics that are separate from those implied by differential, single-ended, and high or low voltage. Table 2-2 on page 33 shows the SCSI terms used to describe different host and device adapters and what they imply in terms of bus width and speed.

Table 2-2 SCSI terms and characteristics

SCSI term	Bus width (bits)	Speed (MB/s)	Max. length	Max. devices
SCSI	8	5	6 m	7
Fast SCSI	8	10	3 m	7
Fast Wide SCSI	16	20	3 m	15
Ultra (Wide) SCSI HVD	16	40	25 m	15
Ultra (Wide) SCSI 2 LVD	16	80	25 m / 12 m	15
Ultra 160 SCSI LVD	16	160	25 m / 12 m	15

Note that a faster bus does not imply that an attached device will support that data rate, but that multiple devices can operate on the bus at that maximum speed. For a detailed table of SCSI terms and related specifications, refer to the SCSI Trade Association Web site at:

`http://www.scsita.org/terms/scsiterms.html`

To ensure best performance, if possible, avoid daisy-chaining.

FC-AL

The first FC-connected tape drives, such as IBM 3590 and IBM Ultrium 1, used Fibre Channel - Arbitrated Loop (FC-AL) attachment. Because IBM tape devices support public loop, those devices were seen in a SAN fabric as regular devices with a WWN, when connected to a switch supporting FC-AL login, such as Brocade and Inrange Switches and Directors.

FC switched fabric - N-Port

Newer tape devices, such as IBM Ultrium 2, use switch fabric connection (N-Port). This eliminates the need for edge loop-switches that support FC-AL login, such as the MC-Data ES1000.

Connector types

When ordering cables, pay careful attention to the type of connector on both the cable and device, so that everything will correctly plug in together. These are the major connector types.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1277
Doc 3698

SCSI HD68

The HD68 connector is the normal 68-pin SCSI connector. All IBM LTO SCSI Drives, except the drives in the 3584, have an HD68 connector. Before June 12, 2001, all LTO tape drives in the 3584 used HD68 connectors.

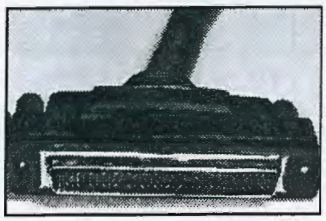


Figure 2-17 HD68 connector

SCSI VHDCI

The VHDCI (Very High Density) connector is a mini-SCSI connector, about half the width of the HD68 connector. All IBM LTO drives in the 3584 have a VHDCI connector.

Figure 2-18 VHDCI connector

FC SC

The duplex SC connector is a low-loss, push/pull fitting connector. The two fibers each have their own part of the connector. The connector is keyed to ensure correct polarization (transmit to receive and vice-versa) when connected. Most 1 Gb SAN devices, including IBM Ultrium 1 FC drives, use SC connectors.

FC LC

Connectors that plug into SFF or SFP devices are called LC connectors. A duplex version is also used so that the transmit and receive are connected in one step. The main advantage of these LC connectors over SC connectors is that they use a smaller form factor and so manufacturers of Fibre Channel components can provide more connections in the same amount of space.

Most 2 Gb SAN devices, including IBM Ultrium 2 FC drives, use LC connectors.

Available interfaces for IBM Ultrium 1

IBM Ultrium 1 drives offer these connection types:

- Ultra2/Wide Low Voltage Differential (LVD) SCSI using VHDCI connector
- Ultra/Wide High Voltage Differential (HVD) SCSI using VHDCI connector
- FC-AL, 1 Gbps using SC connector

Available interfaces for IBM Ultrium 2

IBM Ultrium 2 drives offer these connection types:

- Ultra 160 Low Voltage Differential (LVD) SCSI using VHDCI connector
- Ultra/Wide High Voltage Differential (HVD) SCSI using VHDCI connector
- Switched fabric 2 Gbps using LC connector

2.4.4 Performance

IBM LTO drives provide high performance and will continue to improve with each new generation of products. If you run applications that are highly dependent on tape-processing speed, you can exploit the significant performance provided by the Ultrium tape drives.

IBM Ultrium 1

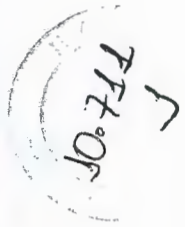
The IBM LTO Ultrium 1 tape drive has these performance characteristics:

- 15 MB/s native sustained data transfer rate
- 30 MB/s sustained data transfer rate at 2:1 compression
- 60 MB/s maximum sustained data rate (at maximum compression)
- 100 MB/s burst data transfer rate for Fibre Channel
- 80 MB/s burst data transfer rate for Ultra-2 SCSI LVD drives
- 40 MB/s burst data transfer rate for Ultra SCSI HVD drives
- 20 s nominal load-to-ready time
- 18 s nominal unload time
- 73 s average search time to first byte of data
- 110 s maximum rewind Time
- 4 m/s read/write speed
- 6 m/s search/rewind speed
- 32 MB buffer

IBM LTO Ultrium drives provide efficient tape operations and relief to users who have difficulty completing tape activities in the time available. If you have limited system backup windows, or if you have large amounts of disk data to back up, Ultrium tape drives are ideal.

By using the built-in data-compression capability of the Ultrium drive, you can potentially achieve greater data rates than the uncompressed data rate.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1278
3698
Doc.



However, the actual throughput is a function of many components, such as the host system processor, disk data rate, block size, data compression ratio, SCSI bus capabilities, and system or application software. Installing multiple tape drives in general (or more than two in the case of IBM LTO) on a single SCSI bus may adversely affect data transfer rates.

IBM Ultrium 2

The IBM LTO Ultrium 2 drives provide more than twice the performance over IBM Ultrium 1 with sustained data rates of 35 MB/s native and 70 MB/s with 2:1 compression. IBM Ultrium 2 has faster load and unload time, faster data access time, faster rewind time, and faster cartridge fill time compared with IBM Ultrium 1.

The IBM LTO Ultrium 2 tape drive has these performance characteristics:

- 35 MB/s native sustained data transfer rate
- 70 MB/s sustained data transfer rate at 2:1 compression
- 110 MB/s maximum sustained data rate (at maximum compression)
- 200 MB/s burst data transfer rate for Fibre Channel
- 160 MB/s burst data transfer rate for Ultra 160 SCSI LVD drives
- 40 MB/s burst data transfer rate for Ultra SCSI HVD drives
- 15s nominal load-to-ready time
- 15 s nominal unload time
- 49s average search time to first byte of data
- 80 s maximum rewind Time
- 6.2m/s read/write speed
- 8m/s search/rewind speed
- 64 MB buffer

2.4.5 Partial Response Maximum Likelihood (PRML)

The IBM patented linear tape implementation of a Partial Response Maximum Likelihood (PRML) channel technology increases linear densities up to 33% and consequently data throughput. The key to PRML's space-saving capability is that on a read-back operation, the magnetic flux transitions are sampled and the sampling feeds logic algorithms that reconstruct the user's data stream, rather than using the flux transitions themselves. The previous method of data encoding was RLL (Run Length Limited) encoding, also patented by IBM for use in earlier tape drives. Figure 2-19 on page 37 compares both methods.

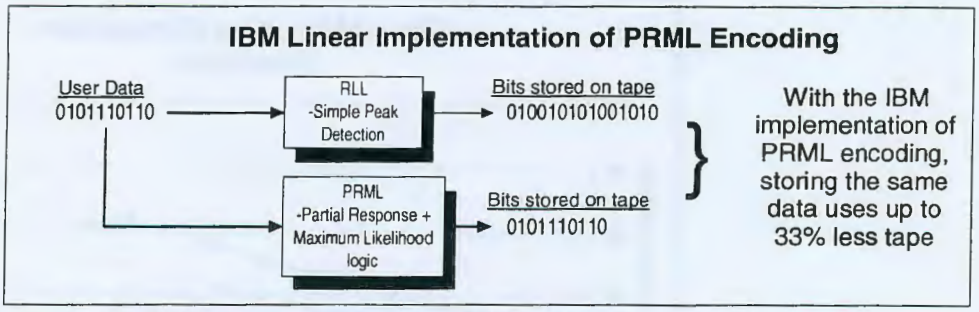


Figure 2-19 IBM linear implementation of PRML encoding

2.4.6 IBM Ultrium 2: additional improvements

On top of the improved performance and capacity, IBM Ultrium 2 provides additional benefits.

Dynamic speed matching

The Ultrium 2 Tape Drive performs dynamic speed matching to adjust the drive's native data rate as closely as possible to the net host data rate (after data compressibility has been factored out). This provides the dual benefit of reducing the number of backhitch repositions and improving throughput performance.

The drive can run in five different speeds: 4/8, 5/8, 6/8, 7/8, and full speed. This results in data transfer rates of 17.5 MB/sec, 21.9 MB/sec, 26.3 MB/sec, 30.6 MB/sec, and 35 MB/sec.

At net host data rates of 17-32 MB/sec, the average throughput performance benefit is 13% when compared with speed matching disabled. At speeds below 17 MB/sec, the drive's 64MB internal buffer masks the performance degradation of repositions. At speeds greater than 32 MB/sec, the drive operates at its fastest possible speed (same speed as speed matching disabled). At net host data rates of 1-32 MB/sec, the average reposition reduction benefit is 68% when compared to speed matching disabled.

Figure 2-20 on page 38 shows the throughput improvement in MB/sec with speed matching enabled relative to speed matching disabled. The statistics show that at each host data rate from 17-32 MB/sec, speed matching enabled improves throughput. Data points from 1-16 and from 33-40 were removed for clarity. At those data points, there is no difference between speed matching enabled vs. disabled as explained in the previous paragraph.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1279
Doc: 3698

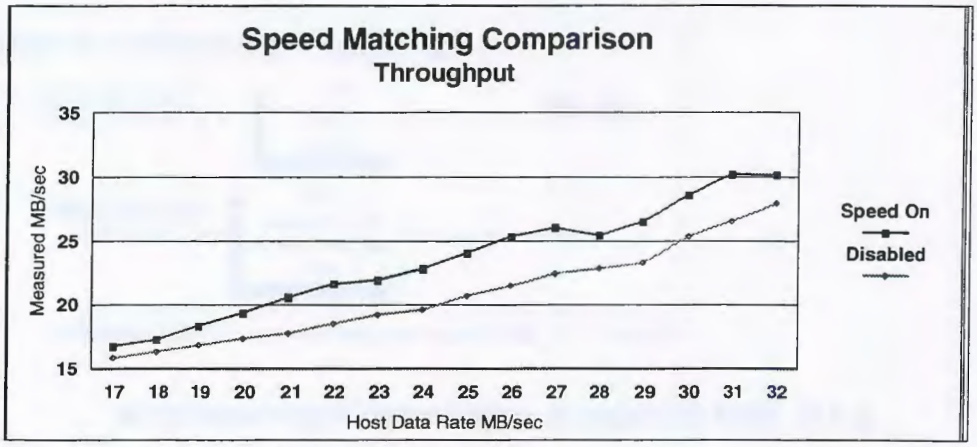


Figure 2-20 Speed matching comparison: MB/sec

If an LTO 1 cartridge is used in an LTO 2 drive, then the LTO 2 drive operates at 5.34 m/sec with no speed matching. While running at 5.34 m/sec, the LTO 2 drive will read and write at 20 MB/sec because of the smaller linear density. There is no need for speed matching when using LTO 1 media, because at the buffer size of 64 MB, the backhitch is transparent. This means that after a start/stop of the drive, the repositioning time is less than the time to fill up the buffer.

Power management

The Ultrium 2 Tape Drive power management function controls the drive electronics to be either completely turned off or to be in a low-power mode. These power modes occur only when the circuit functions are not needed for drive operation.

Channel calibration

The Ultrium 2 tape drive channel calibration feature allows for customization of each read/write data channel for optimum performance. The customization enables compensation for variations in the recording channel transfer function, media characteristics, and read/write head characteristics.

Separate writing of multiple filemarks

Separate writing of multiple filemarks means that any write command of two or more filemarks will cause a separate data set to be written containing all filemarks after the first. This feature has two advantages. First, it improves performance if a subsequent append overwrites somewhere after the first filemark. Second, writing multiple filemarks typically indicates a point where an append operation might occur after the first of these filemarks. This change

prevents having to rewrite datasets containing customer data and the first filemark if such an append occurs.

2.4.7 IBM Ultrium 1 and 2 compatibility

IBM Ultrium 2 tape drives (both standalone and in IBM Ultrium libraries) support both Ultrium 1 and Ultrium 2 cartridges. An Ultrium 1 cartridge in an Ultrium 2 drive will be written at the same 100 GB native capacity, but with improved performance (20 MB/s). Ultrium 1 drives cannot read or write an Ultrium 2 cartridge. If you put an Ultrium 2 cartridge in an Ultrium 1 drive, then you will get an "Unsupported Cartridge Format" failure. Figure 2-21 shows the compatibility.

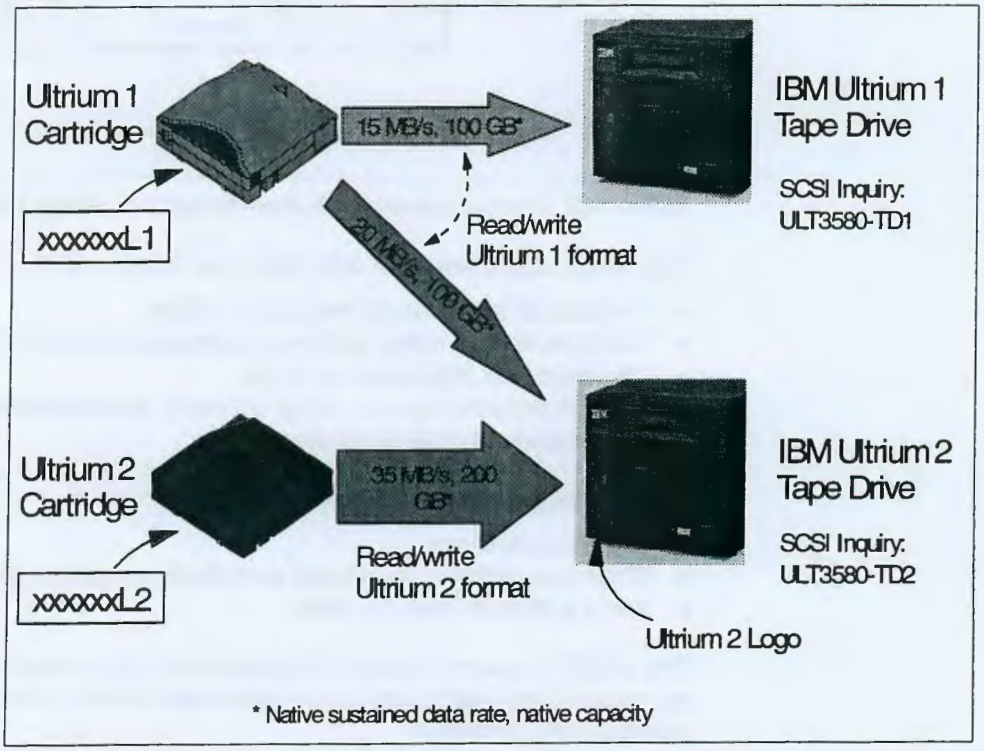


Figure 2-21 IBM Ultrium 1 and 2 compatibility

2.4.8 Operating the Ultrium drive

The IBM subassembly itself has a simple status LED indicator, an unload push button, and a single-character display (see Figure 2-22 on page 40).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1280
3698
Doc.

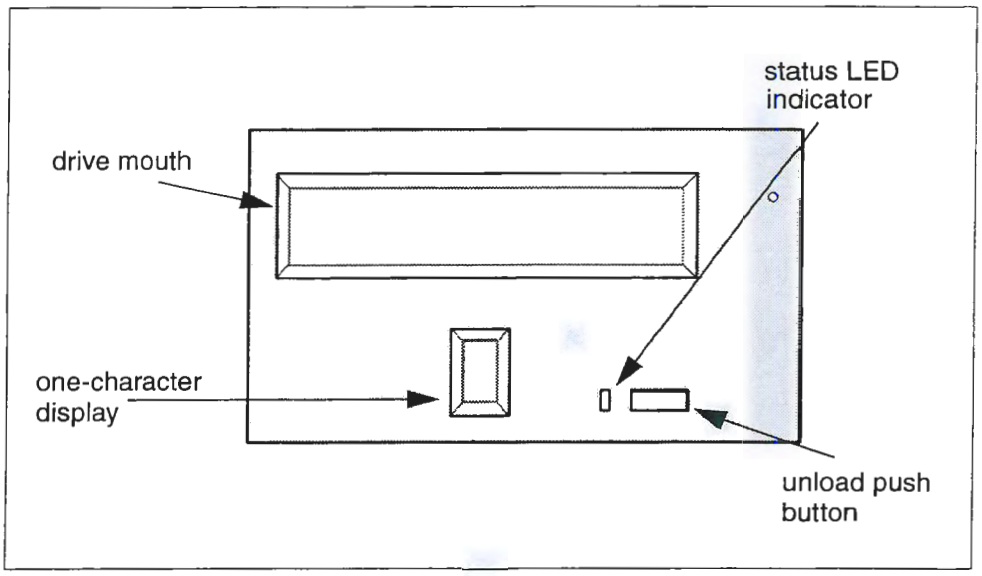


Figure 2-22 Front of subassembly showing operator panel indicators

The status LED uses color and lighting to indicate that:

- The tape is in motion for reading or writing.
- The drive is rewinding, locating, or unloading the cartridge.
- The drive is in maintenance mode.
- A failure occurred and the drive or media requires service.
- A microcode update is occurring.

The unload push button enables the operator to:

- Unload a cartridge
- Enter maintenance mode and execute maintenance operations
- Force a drive dump operation

The single-character display indicates errors and communicates messages, such as requests for cleaner tapes. It is also used by the operator for diagnostic and maintenance functions.

10.706
3

2.4.9 Reliability

The IBM LTO Ultrium tape format differs from earlier IBM products. Reliability and availability features include:

- Data integrity

  The drive performs a read after write, for verification. Incorrectly written data, such as the result of a tape defect, is automatically rewritten by the drive in a new location. Data rewritten as the result of media defects is not counted against the drive error performance.

  The drive will never record incorrect data to the tape media without posting an error condition.

- Power loss

  No recorded data is lost as a result of normal or abnormal power loss while the drive is reading or writing data. If power is lost while writing data, only the data block currently being written may be in error. Any previously written data will not be destroyed.

- Error correction

  Data integrity features include two levels of error correction that can provide recovery from longitudinal media scratches.

- Integrated head cleaner

  The head of the drive must be kept clean to prevent errors caused by contamination. During the load process, a brush integrated into the drive mechanism cleans the head before it is used with the tape. This keeps the head and media free of debris on a continuing basis and is expected to lead to less requirement for drive-cleaning operations.

- Surface control guiding

  IBM's patented Surface Control Guiding Mechanism guides the tape along the tape path using the surface of the tape rather than the edges to control tape motion. Through grooved rollers (see Figure 2-23 on page 42), an air cushion builds between the tape and the rollers that keep it in the right position. This results in less tape damage (especially to the edges of the tape) and less debris from damaged edges that can accumulate in the head area, and helps minimize the chance of physical damage to the tape media.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 1281
3698
Doc.

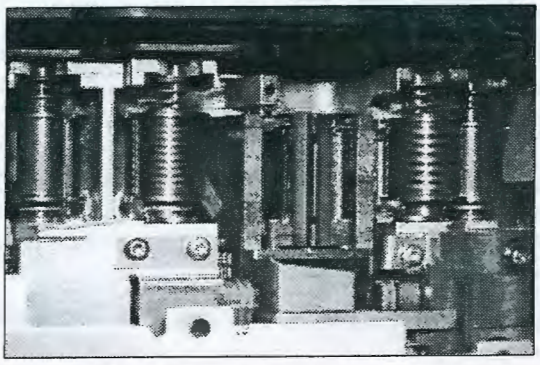


Figure 2-23 Surface control guiding

- Flat lap head

  The flat head improves contact between the read and write recording elements and the tape, giving higher quality recording and readback of data.

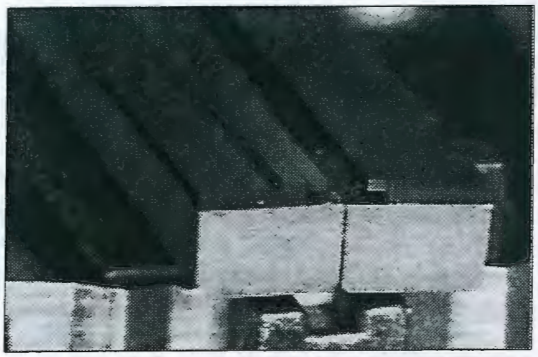


Figure 2-24 Flat lap head

Surface control guiding and the flat lap head are designed to help minimize debris generated as the tape moves through its path, resulting in increased reliability in reading and writing data. This also potentially increases the life expectancy of the media by not using the edges of the tape to guide it over the read/write head. Historically, this also was a major source of debris on the tape path.

- Statistical Analysis and Reporting System

  Statistical Analysis and Reporting System (SARS) is another IBM exclusive. Only IBM LTO drives provide this level of preventive diagnostic reporting. The Ultrium drive uses this reporting system to assist in isolating failures between media and hardware. SARS uses the cartridge performance history saved in the CM module and the drive performance history kept in the drive flash

EEPROM to determine the most likely cause of failure. It then can cause the drive to request a cleaner tape, to mark the media as degraded, and to indicate that the hardware has degraded. SARS reports the results of its analysis in the form of Tape Alert if needed (see Figure 2-25).

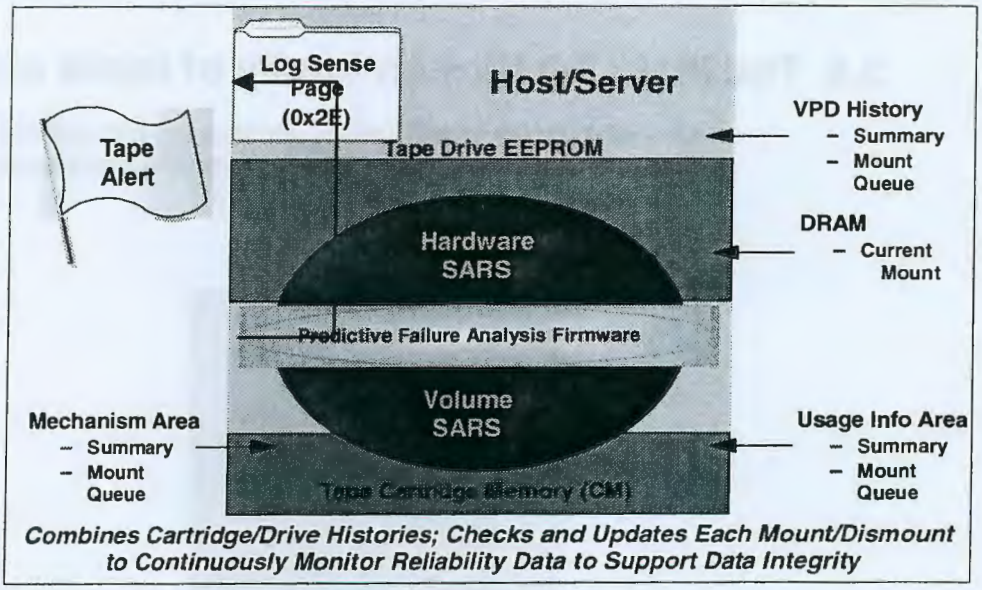


Figure 2-25 Statistical Analysis and Reporting System

2.4.10 Cleaning the drive

In addition to the integrated head-cleaning mechanism, IBM recommends that the drive be cleaned regularly, with automatic cleaning enabled where supported in the libraries. Regular cleaning avoids drive shutdowns because of improper maintenance or contaminants that cause the drive to fail.

In the unusual event that the drive head becomes clogged, it *may* be necessary to use the specially labeled IBM LTO Ultrium cleaning cartridge supplied with each Ultrium tape drive product. The cleaning cartridge is good for 50 cleaning operations. If cleaning proves necessary, the LTO-CM memory in a cleaning cartridge is used to track the number of times that the cartridge has been used. After the cartridge has been used 50 times, the drive will mark the cleaning cartridge as expired. This also protects you from accidentally reinserting a cleaning cartridge that has been used 50 times.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1282
Doc. 3698

Note: The use of cleaning cartridges is not necessary (and is discouraged) for normal operation of Ultrium tape drives. See *3580 Ultrium Tape Drive Setup, Operator, and Service Guide*, GA32-0415, for information about drive cleaning.

2.5 The IBM LTO Ultrium family of tapes and libraries

The IBM Ultrium family of tapes and libraries (pictured in Figure 2-26) comprises five different product offerings, ranging from a stand-alone unit to a highly scalable automated library.

Figure 2-26 The IBM Ultrium family of tapes and libraries

They are all based on a common tape drive subassembly packaged in different robotic and stand-alone environments.

- The *IBM TotalStorage Ultrium Tape Drive 3580* is a stand-alone desktop single-drive unit without autoloader. Tapes are mounted manually one at a time.
- The *IBM TotalStorage Ultrium Tape Autoloader 3581* is also a single-drive unit, but it has a seven-cartridge autoloader within the device. It is a stand-alone desktop unit; however, optional additional hardware is available for installation in a standard 19-inch rack.
- The *IBM TotalStorage Ultrium Tape Library 3582* is a small robotic library, accommodating one to two drives and providing space for up to 23 Ultrium cartridges. The IBM 3582 may be stand-alone or, with an optional feature, housed in a rack.
- The *IBM TotalStorage Ultrium Scalable Tape Library 3583* is a small robotic library, accommodating from one to six drives and providing space for up to 72 Ultrium cartridges. The IBM 3583 may be standalone or, with an optional feature, housed in a rack.
- The *IBM TotalStorage UltraScalable Tape Library 3584* is a larger modular library with the potential to house a maximum of 192 tape drives in as many as 16 frames. There is a trade-off between cartridge capacity and installed drives, so that a fully-configured library with 192 drives and a 10-cartridge I/O station has a cartridge capacity of 6167; with a minimal drive configuration the cartridge capacity can reach a maximum of 6881.

Storage and tape management for the IBM LTO Ultrium family is provided by software such as IBM Tivoli Storage Manager and other similar software offerings.

These products, while all part of the same family, are distinct offerings. The drive and cartridge technology and formats are the same, and the cartridges are interchangeable between the libraries, as dictated by the LTO format standards. However, the machine types (for example, 3583 and 3584) are not upgradeable from one to another, nor can the Ultrium drives be exchanged between different libraries. Thus, if you purchase an IBM 3583 with six drives and later on install an IBM 3584, you cannot transfer the Ultrium drives from the 3583 to the 3584.

Detailed descriptions of these products can be found in Chapter 4, "IBM TotalStorage Ultrium Tape Drive 3580" on page 79, through Chapter 8, "IBM TotalStorage UltraScalable Tape Library 3584" on page 159.

The IBM LTO family of products is sold directly through IBM and its Business Partners.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1283
Doc: 3698

2.6 Multi-path architecture

This patented multi-path architecture was introduced with the IBM Magstar MP 3575 library. It provides a way to share a tape library between a number of servers without the need to implement application software to control and serialize tape drives and media. It is also implemented in the IBM 3582, 3583, and 3584 libraries.

Multi-path architecture is an IBM unique feature. The IBM 3582, 3583, and 3584 LTO libraries feature the second generation of the architecture introduced with the Magstar MP 3575 library. It uses the SCSI-3 Move Media command set that is featured in midrange and open libraries. The key benefit is that multi-path architecture removes the need for a dedicated server plus middleware to control the use of a library by many different hosts utilizing different operating systems, as each drive has its own path to the control unit.

Conventional tape libraries use a dedicated host port to communicate to the library, such as to send mount request commands. IBM LTO tape libraries use the same path to communicate with both the drives and the library controller, as shown in Figure 2-27. This is not one dedicated path, but it may be any path to any tape drive.

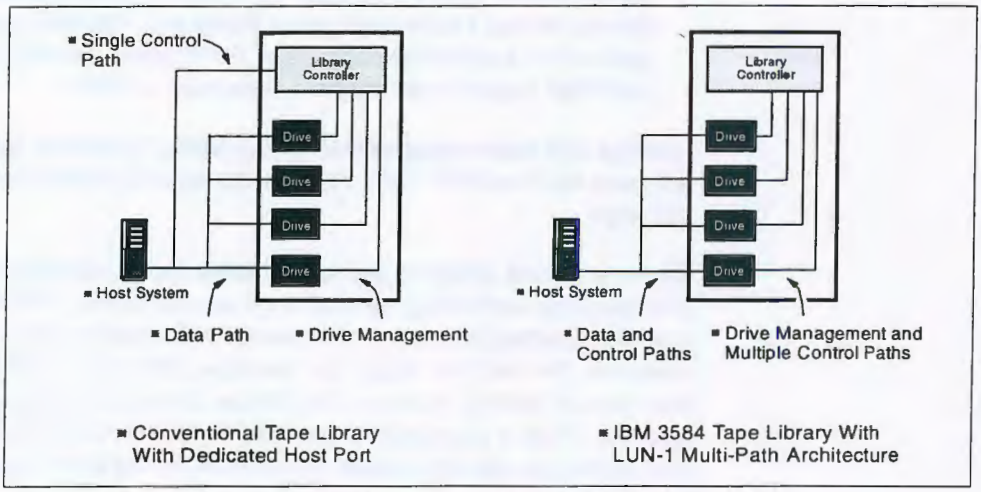


Figure 2-27 Conventional tape library vs. multi-path architecture

For conventional tape libraries, the control path is a single point of failure. In contrast, the IBM LTO tape libraries offer as many control paths as there are drives installed in the library, so in the event of individual control path failure you can communicate with your library over different, redundant control paths. As shown in Figure 2-28 on page 47, if one path to a drive is broken because of a

defective switch port, cable, or HBA, communication to the library controller can still occur using one of the other available paths. In conjunction with automatic Control Path Failover, this constitutes a unique high-availability option.

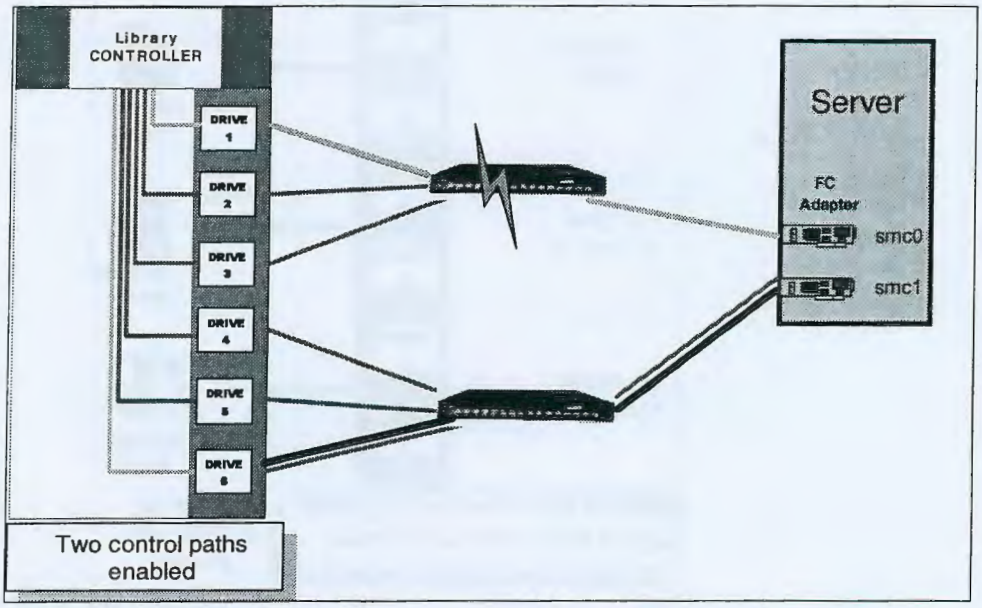


Figure 2-28 Redundant control paths to the library controller

As well as the redundant control path, multi-path architecture offers the additional benefit of built-in partitioning. With the partitioning feature of the IBM LTO libraries, you can divide the physical library into several smaller logical libraries, which are independent from each other. The maximum number of logical libraries varies by model type. A logical library must contain at least one tape drive and can comprise more than one tape drive sharing the same cartridge cells.

With this partitioning option, the library can be shared between multiple heterogeneous hosts. Each logical library has its own drives, cartridges, and control paths. Because of barriers between the logical libraries, cartridges cannot be moved from one logical library to another. Figure 2-29 on page 48 shows three logical libraries with two drives each and some cartridge storage slots dedicated to each of the heterogeneous servers.

RQS nº 03/2005 - CN
CPMI CORREIOS
Nº 1284
Doc: 3698

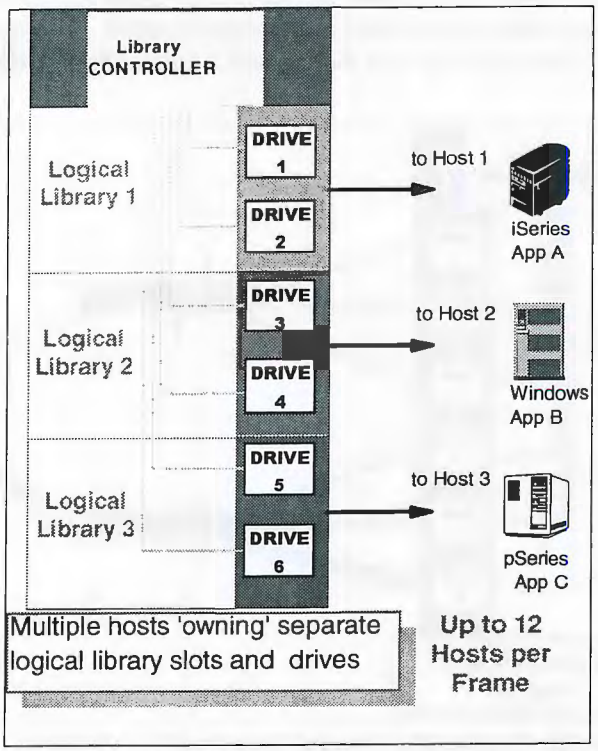
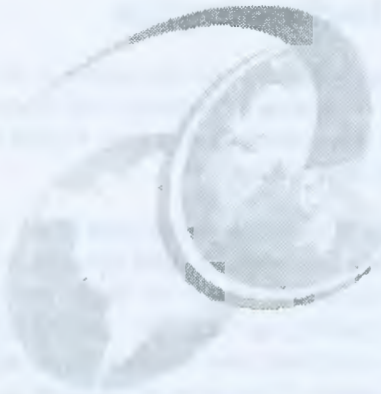


Figure 2-29 IBM LTO tape library partitioned into three logical libraries

10.698



3

Tape storage market direction

Tape systems traditionally have been associated with the mainframe computer market, because they have represented an essential element in mainframe systems architectures since the early 1950s as a cost-effective way to store large amounts of data. The mid-range and client/server computer market has, in contrast, made very limited use of tape technology until quite recently.

Over the past few years, however, the growth in the demand for data storage and reliable backup and archiving solutions has greatly increased the need to provide manageable and cost-effective tape library products. The value of using tape for backup purposes hasonly gradually become obvious and important in these environments.

In this chapter, we will review the technologies, formats, and standards that you will see for tape products in today's market. We discuss a number of products from non-IBM vendors and, although we have reviewed the material carefully, we would remind you that the vendors of those products are the definitive source of information.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CEMI - CORREIOS
Fls Nº 1285
3698
Doc

3.1 Current tape products and technologies

Two basic tape technologies have been utilized. Until the middle of the 1980s, all computer tape systems utilized linear recording technology, a technology that uses a stationary head writing data in a longitudinal way (see Figure 3-3 on page 54 for an example of longitudinal technology).

In the middle of the 1980s, helical tape technology (which had been developed for video applications) became available for computer data storage, a technology that uses heads rotating on a drum and writing data in an angle. Helical tape systems found natural applications in backing up magnetic disk systems where their cost advantages substantially outweighed their operational disadvantages (see Figure 3-4 on page 55 for an example of helical-scan technology).

3.1.1 Helical versus longitudinal

The first computer tape systems used linear recording technology. This technology provides excellent data integrity, rapid access to data records, and reasonable storage density.

The first implementation of linear recording technology used magnetic tapes on open reels. Later, the tape was protected inside cartridges, using one or two reels. Linear technology drives write each data track on the entire length of the tape. Data is first written onto a track along the entire length of the tape, and when the end is reached, the heads are repositioned to record a new track again, along the entire length of the tape, now travelling in the opposite direction. This continues back and forth until the tape is full. On linear drives, the tape is guided around a static head.

On helical scan systems, by contrast, the tape is wrapped around a rotating drum containing read/write heads. Due to the more complicated path, mechanical stress is placed on the tape. When contrasted with linear tape systems, helical tape systems have higher density (and, therefore, lower media cost), but lower data transfer rates (due to the smaller number of active read/write heads), less effective access to random data records, increased maintenance requirements, and reduced data integrity.

Both linear and helical tape systems have advanced substantially over the past decade. Linear systems have improved significantly in the areas of storage density (and, therefore, cost), and operational convenience (with a variety of removable cartridge systems such as 3590, QIC, DLT, and now LTO replacing reel-to-reel systems). Helical systems have improved in the areas of transfer rate and data integrity with the implementation of both channel and error correction coding technologies.

Over the past few years, one of the most significant advances in tape technology for computer applications has been the maturation of serpentine linear recording systems which, for the first time, has permitted linear recording systems to provide recording density that is comparable with that of helical systems. The first commercially successful serpentine linear tape system for professional applications was DLT. Another important improvement is the use of servo tracks, first introduced by IBM on the Magstar 3590 tape. Servo tracks on the tape cartridge are recorded at the time of manufacture. These tracks enable the tape drive to position the read/write head accurately with respect to the media while the tape is in motion.

Most linear media is manufactured using metal particle (MP) technology. As with most tape products, metal particle media comprises several layers: a substrate that provides the base for other layers, the magnetic layer where data is stored, and a back coat that controls the media's frictional characteristics.

The most advanced implementations of 8 mm format (Mammoth and AIT) use AME (Advanced Metal Evaporative) media. The AME magnetic layer is 100% cobalt and is a much thinner, pure magnetic layer that doesn't contain any binders or lubricants. These qualities give AME tapes greater potential data density so that more information can be stored on less tape surface.

Future generations of linear tape media (including LTO) will use the same AME magnetic layer technology, offering increased data densities.

We felt that the fundamental difference between linear recording and helical scan technologies is so important that it would be worthwhile to summarize all of the available current technologies (see Table 3-1).

Table 3-1 Tape technology overview

Name	Recording technology	Media width	Type
1/2-inch reels	linear	1/2 inch	single hub
QIC	linear	1/4 in and 8 mm	dual hub
DAT/4 mm	helical-scan	4 mm	dual hub
DDS	helical-scan	all 4 mm	dual hub
8 mm	helical-scan	8 mm	dual hub
Mammoth	helical-scan	8 mm	dual hub
AIT	helical-scan	8 mm	dual hub
Ecrix VXA	helical-scan	8 mm	dual hub

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1286
3698
Doc.

Name	Recording technology	Media width	Type
DLT	linear	1/2 inch	single hub
IBM 3480/90	linear	1/2 inch	single hub
IBM Magstar MP 3570	linear	8 mm	dual hub
IBM Magstar 3590	linear	1/2 inch	single hub
STK 9840	linear	1/2 inch	dual hub
STK 9940	linear	1/2 inch	dual hub
LTO Ultrium	linear	1/2 inch	single hub

3.1.2 Tape reels (1/2-inch)

The first data backup device (and the ancestor of magnetic tape devices with a 1/2-inch-wide tape format) used magnetic tape reels, shown in Figure 3-1. Reel tapes have been around for many years. They can support densities from 800 bpi to 6250 bpi (bits per inch) and were manufactured and sold in many different lengths and brands. The most common densities used were 1600 and 6250 bpi, but most of these devices have been replaced today.

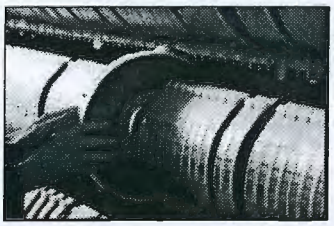


Figure 3-1 Tape reels, 1/2-inch

3.1.3 QIC

The quarter-inch-tape cartridge (QIC) was first introduced in 1972 by the 3M company as a means to store data from telecommunications and data acquisition applications. As time passed, the comparatively inexpensive QIC drive became an accepted data storage system, especially for stand-alone PCs.

QIC cartridges (shown in Figure 3-2 on page 53) look much like audio tape cassettes with two reels inside, one with tape and the other for take-up. The reels are driven by a belt built into the cartridge. A metal rod, known as a capstan, projects from the drive motor and pinches the tape against a rubber drive wheel.

10.694

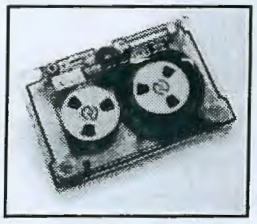


Figure 3-2 QIC cartridge

The QIC format employs a linear (or longitudinal) recording technique in which data is written to parallel tracks that run along the length of the tape. The number of tracks is the principle determinant of capacity. The cartridges come in two varieties, DC600 cartridge and DC2000 mini cartridge, the latter being the more popular. The encoding method used is either MFM (Modified Frequency Modulation) or RLL (Run Length Limited), and is similar to the way a hard drive encodes data.

When a backup is started, directory information from the file allocation table is loaded into a memory buffer in the system's RAM, along with the appropriate files. Both sets of data are sent to the tape drive controller, each file being prefaced by a header containing the directory information. If the controller has built-in error correction, an error correction code (ECC) is appended to the data in the controller. Otherwise, the software adds the code before sending the data to the controller.

The controller contains its own buffer. Once the backup data containing the ECC is in this buffer, the backup software is free to load more data into system memory. The drive's controller then sends the data as required to the tape drive mechanism.

QIC uses a linear read/write head similar to those found in domestic cassette recorders (Figure 3-3 on page 54). The head contains a single write head flanked on either side by a read head. This allows the tape drive to verify data just written when the tape is running in either direction. If the data just written is verified by the read head, the buffer is flushed out and new data is acquired from the system memory.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1287
3698
Doc.

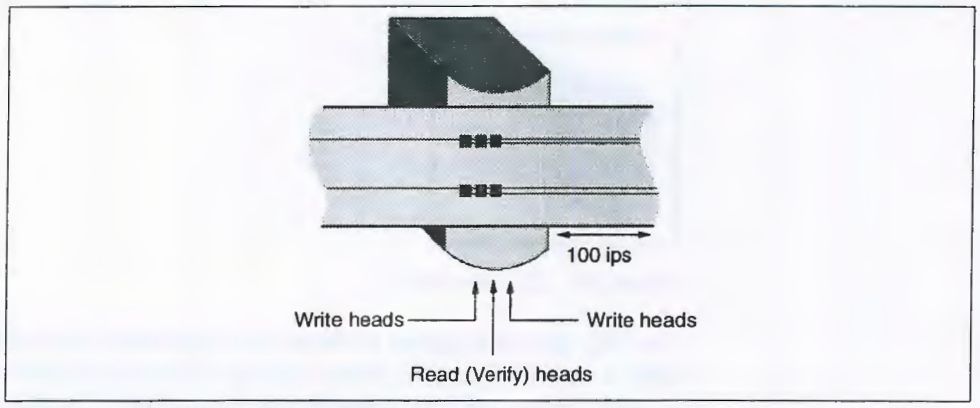


Figure 3-3 QIC head diagram

QIC standards

As the QIC standards of the time failed to keep up with the storage media explosion of the mid-1990s, the QIC cartridge underwent an evolution that increased capacities by both lengthening and widening the tape. The Sony-inspired move to a wider format tape was a noteworthy development.

One of the drawbacks with QIC is incompatibility. The format has suffered from an overabundance of standards over the years—there are more than 120 currently—and not all QIC drives are compatible with all standards.

Tandberg Data remains the only drive manufacturer in this segment with its Scalable Linear Recording (SLR) technology. Their most recent drive, the SLR100, provides 50 GB (native) and 100 GB (with 2:1 compression) capacity on a single data cartridge. The maximum data transfer rates are 5 MB/s uncompressed and 10 MB/s (with 2:1 compression).

3.1.4 Digital Data Standard (4 mm)

The Digital Audio Tape (DAT) standard was created in 1987 and, as its name implies, was originally conceived as a CD-quality audio format offering three hours of digital sound on a single tape. The Digital Data Standard (DDS) is based on DAT and uses a similar technology. The cartridge design is common, but different tape formulations have been developed. In 1988, Sony and HP defined the DDS standard, transforming the format into one that could be used for digital data storage.

DAT technology is a 4 mm tape that uses helical scan recording technology. This is the same type of recording as that used in videocassette recorders and is inherently slower than the linear type. The tape in a helical scan system is pulled

from a two-reel cartridge and wrapped around a cylindrical drum containing two read heads and two write heads, arranged alternately. The read heads verify the data written by the write heads. The cylinder head is tilted slightly in relation to the tape and spins at 2,000 revolutions per minute. The tape moves in the opposite direction to the cylindrical spin, at less than one inch per second, but because it is recording more than one line at a time it has an effective speed of 150 inches per second (refer to Figure 3-4).

Short diagonal tracks, about eight times longer than the width are written across the width of the tape. These each contain about 128KB of data and an error correction code.

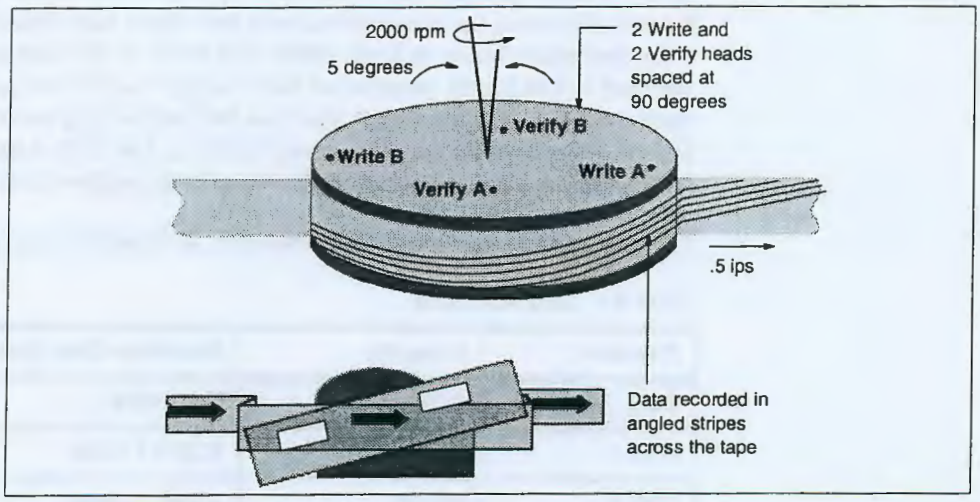


Figure 3-4 Helical-scan recording diagram

A read head verifies the data. If errors are present the data is rewritten; otherwise the controller buffer is flushed ready for the next segment. The second write head writes data at a 40-degree angle to the first one.

Even though the first and second writes overlap, they are magnetically encoded with different polarities so they are only read by the correct read head. The "criss-cross" pattern packs more data onto the tape, enabling helical scan systems to achieve very high data densities. A directory of files is stored in a partition at the front of the tape.

Just as with linear recording, the performance would be greatly improved if additional read/write heads were added, but this is difficult with helical scan devices, because of the design of the rotating head. The fact that the heads may only be added in pairs makes it difficult to fit the wiring inside a single cylinder, and this limits the potential performance of helical scan devices. Because of the

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1288
3698
Doc.

wide wrap angle of the tape and the consequent degree of physical contact, both the head and the media are prone to wear and tear.

When restoring from the backup, the backup software first reads the entire directory of the tape's contents. It then winds the tape to the appropriate spot and reads the contents into the controller's buffer. The controller uses the CRC code to make sure the information is correct. If errors are detected, the ECC can be used to fix them. Once the data has been verified as correct, the buffer contents are passed to system memory.

DDS-3 uses the same helical scanning head but adds a technology commonly used for hard disk drives, called PRML (Partial Response, Maximum Likelihood), which is used to weed out the data from electronic noise. The latest DDS-4 format, proposed by Hewlett-Packard and Sony, was endorsed by the DDS Manufacturers Group in April 1998. The extra 16 GB compressed capacity realized in this fourth-generation technology is achieved by reducing the track pitch from 9.1 microns to 6.8 microns and increasing the length of the media to 150 m. As with previous DDS specifications, the DDS-4 standard provides backward read and write compatibility with the earlier formats.

Table 3-2 shows current DDS standards, all of which are backward-compatible.

Table 3-2 DDS standards

Standard	Capacity	Maximum Data Transmission Rate
DDS	2 GB	0.55 MB/s
DDS-1	2/4 GB	0.55/1.1 MB/s
DDS-2	4/8 GB	0.55/1.1 MB/s
DDS-3	12/24 GB	1.1/2.2 MB/s
DDS-4	20/40 GB	2.4/4.8 MB/s

3.1.5 The 8 mm format

Designed for the video industry, 8 mm tape technology was created to transfer high-quality color images to tape for storage and retrieval and now has been adopted by the computer industry. Similar to DAT, but with greater capacities, 8 mm drives are also based on the helical scan technology. A drawback to the helical scan system is the complicated tape path. Because the tape must be pulled from a cartridge and wrapped tightly round the spinning read/write cylinder (Figure 3-5 on page 57), a great deal of stress is placed on the tape.

10.690

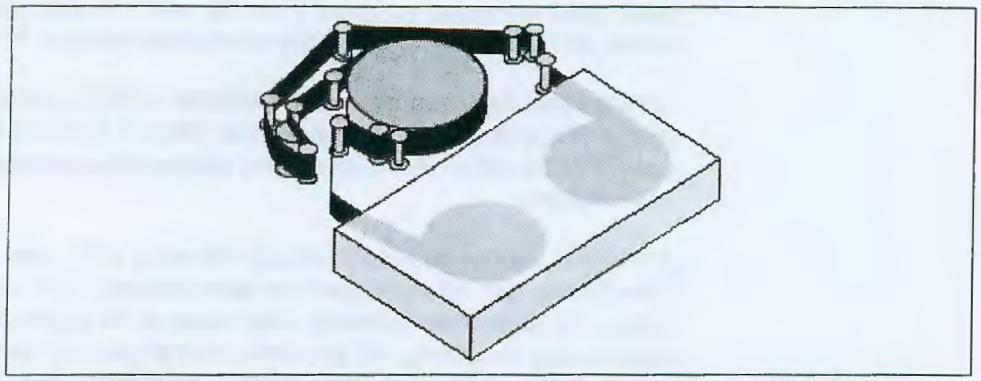


Figure 3-5 An 8 mm tape path

There are two major protocols that use different compression algorithms and drive technologies, but the basic function is the same. Exabyte Corporation sponsors standard 8 mm and Mammoth formats, while Seagate and Sony represent a new 8 mm technology known as Advanced Intelligent Tape (AIT).

Mammoth tape format

This is a SCSI-based 8 mm tape technology, designed for open system applications. It is a proprietary implementation of the 8 mm standard format available since 1987 and uses Advanced Metal Evaporative (AME) media. This media has a coating over the recording surface that seals and protects the recording surface.

The Exabyte Mammoth tapes have an 3.5-inch form factor. The first generation provide 20 GB (native) and 40 GB (with 2:1 compression) capacity on a single 8 mm data cartridge. The maximum data transfer rates were 3 MB/s uncompressed and 6 MB/s (with 2:1 compression).

With the Mammoth-2 technology the capacity and data rate have been increased to 60 GB (120 GB with 2:1 compression) and 12 MB/s uncompressed (24 MB/s with 2:1 compression). Mammoth-2 drives are read compatible with the previous models.

Advanced Intelligent Tape (AIT) format

The AIT format was developed by Sony. Available in a 3.5-inch form factor, Sony's AIT-1 drives and media provide 25 GB (native) and 50 GB (with 2:1 compression) capacity on a single 8 mm data cartridge. The maximum data transfer rate is 3 MB/s native.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1289
3698
Doc.

With the AIT-2 technology made available in 1999, the capacity and data rate have been increased to 50 GB (100 GB with 2:1 compression) and 6 MB/s native. AIT-2 drives are backward-compatible with the AIT-1models.

Sony's latest AIT-3 format, made available in 2001, doubles the capacity and performance of the prior generation to 100 GB (200 GB with 2:1 compression) and 12 MB/s native. AIT-3 drives are backward-compatible with the AIT-2 and AIT-1 models.

AIT drives feature an Auto Tracking Following (ATF) system, which provides a closed-loop, self-adjusting path for tape tracking. This servo tracking system adjusts for tape flutter, allowing data tracks to be written much closer together for high-density recording. AIT provides Fast/Wide SCSI technology with data transfer rates of up to 12 MB/s (native), 24.0 MB/s (with 2:1 compression). AIT uses the Adaptive Lossless Data Compression technology (ALDC) compression algorithm. The 8 mm standard has various drive generations, all of which are backward-compatible, shown in Table 3-3.

Table 3-3 Standards for 8 mm

Standard	Capacity	Maximum Data Transmission Rate (compressed)
Standard 8 mm	3.5/7 GB	0.53 MB/s
Standard 8 mm	5/10 GB	1 MB/s
Standard 8 mm	7/14 GB	1 MB/s
Standard 8 mm	7/14 GB	2 MB/s
Mammoth	20/40 GB	6 MB/s
Mammoth-2	60/120 GB	24 MB/s
AIT-1	25/50 GB	6 MB/s
AIT-2	50/100 GB	12 MB/s
AIT-3	100/200 GB	24 MB/s

3.1.6 Digital Linear Tape (DLT)

DLT drives appeared in 1985 when Digital Equipment Corporation needed a backup system for their MicroVAX systems.

The system uses a square cartridge that contains tape media but no take-up reel. The take-up reel was built into the drive itself. This design eliminated the additional space typically associated with cassette and cartridge drives such as

QIC or 8 mm. The drive itself had to be made larger than most to accommodate the internal take-up reel. Called the TK50, the new tape drive was capable of storing 94 MB per cartridge.

Using a ferrite read/write head, the TK50 recorded data in linear blocks along 22 tracks. The TK50's read/write head actually contained two sets of read/write elements. One set was used when reading and writing forward, and the other when reading and writing backward.

The TK50 started recording at the beginning of the tape, recording on one track. When it reached the end, the system recorded back to the beginning along a new track. After every two tracks that were written, the system moved the head up the width of one track and began the process again. The read-after-write capability of the system ensured basic data accuracy. The drive fit into a full-height, 5.25" drive bay.

In 1987, Digital released the TK70. This tape drive offered 294 MB of storage on the same square tape cartridge, a threefold improvement over the TK50. This was accomplished by increasing the number of tracks to 48 and by increasing density on the same 1/2-inch tape.

In 1989, Digital introduced the TF85, the first true DLT system. The TF85 (later to be called the DLT 260) incorporated a new feature that enabled the system to pack 2.6 GB onto a 1,200-foot tape (CompacTape III, now known as DLTtape III).

The DLT Tape Head Guide Assembly was incorporated for the first time in the TF85 drive. Six precision rollers provided long tape life. The six-roller head guide assembly gave the TF85 a much shorter tape path than helical-scan systems (Figure 3-6).

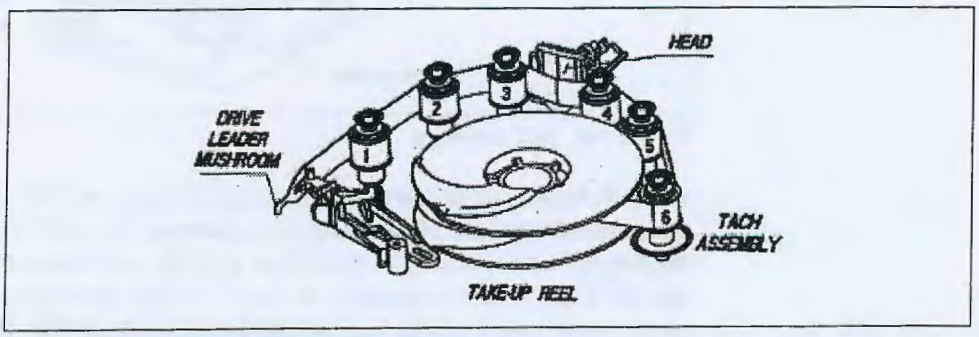


Figure 3-6 DLT tape path mechanism

The read/write head was equipped with an additional write element. The elements now were arranged in a write/read/write pattern. This pattern enabled

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1290
3698
Doc.

the TF85 to read after writing on two channels and in both forward and reverse directions. This is the multi-channel serpentine recording depicted in Figure 3-7.

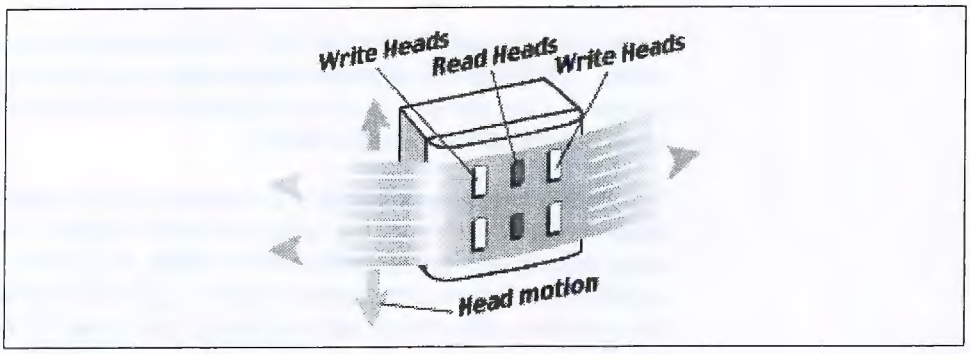


Figure 3-7 DLT 2000 recording head design

Two years later, Digital introduced the TZ87, now known as the DLT 2000 tape drive. This system offered 10 GB of native capacity on a single CompacTape III cartridge (shown in Figure 3-8) and now known as DLTtape III, 2 MB of read/write data cache memory, and a data transfer rate of 1.25 MB/s. This was the first generation of DLT.

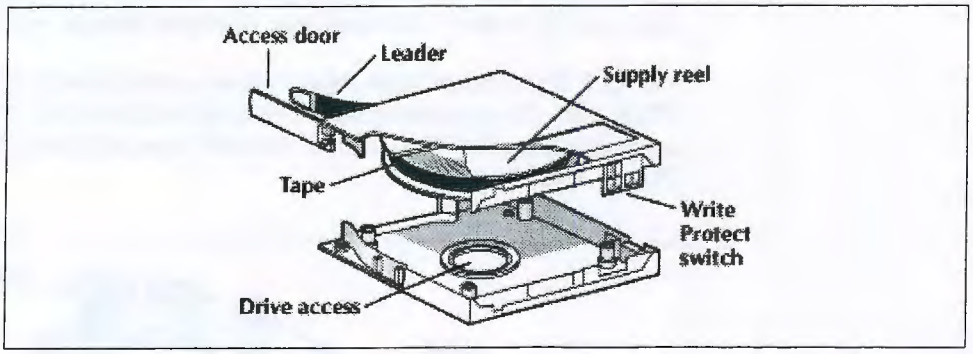


Figure 3-8 DLT cartridge

In 1994, Quantum acquired the Storage division of DEC (Digital Equipment Corporation). In late 1994, Quantum released the DLT 4000. By increasing real density (bits per inch) from 62,500 to 82,000, and tape length by 600 additional feet (DLTtape IV), the capacity of the DLT 4000 grew up to 20 GB (40 GB compressed) on a single 1/2-inch DLTtape IV cartridge. The new DLTtape system provided data transfer at 1.5 MB/s (3 MB/s compressed) and was fully read/write compatible with previous generations of DLTtape drives.

DLT 2000 and DLT 4000 drives write data on two channels simultaneously in linear tracks that run the length of the tape, as shown in Figure 3-9 on page 61.

10.686

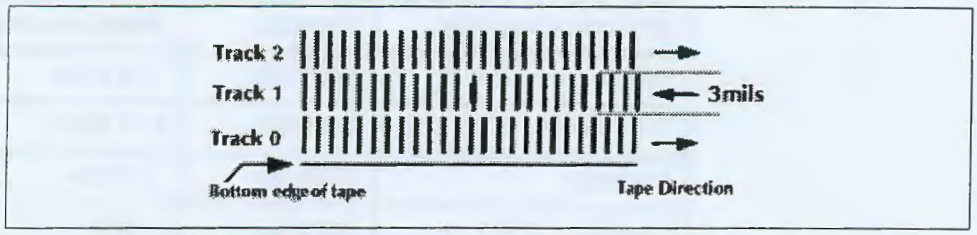


Figure 3-9 DLT 2000/4000 linear recording format

The DLT 7000 appeared in 1996. This drive offered a total storage capacity of 35 GB native, 70 GB compressed on the 1,800 foot DLTtape IV cartridge. The DLT 7000 incorporated a 4-channel head that gives the drive a transfer rate of 5 MB/s of data in native mode (Figure 3-10).

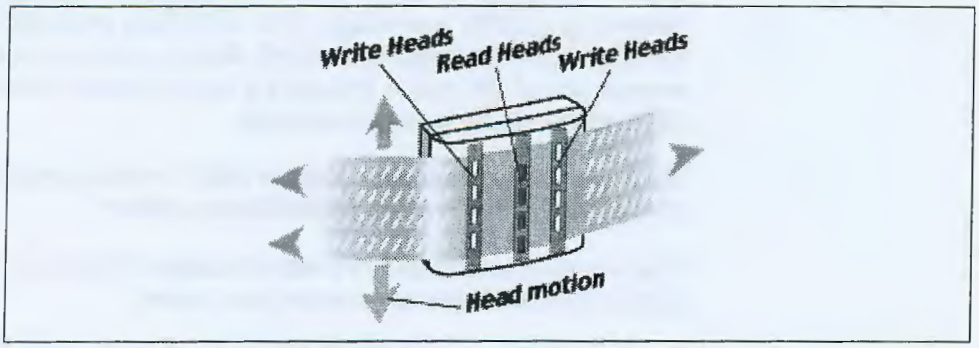


Figure 3-10 DLT 7000/8000 tape head

Quantum's latest DLT product is their DLT 8000 drive. This tape drive features a native transfer rate of up to 6 MB/s, with a native capacity of 40 GB. The DLT 7000/8000 drives incorporate the Symmetric Phase Recording technology that writes data in an angled pattern (Figure 3-11).

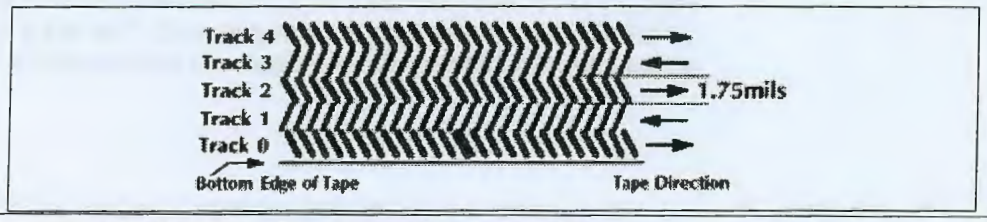


Figure 3-11 Symmetric Phase Recording technology

The DLT standard has various generations of tape drive, all of which are backward-compatible. We have summarized the specifications in Table 3-4 on page 62.

RQS nº 03/2005 - CN
CPMI CORREIOS
Nº 1291
Doc. 3698

10.685

Table 3-4 DLT drive standards

DLT drive generation	Capacity	Maximum data transmission rate
DLT2000	10/20 GB	1.25 MB/s
DLT2000XT	15/30 GB	1.25 MB/s
DLT4000	20/40 GB	1.5 MB/s
DLT7000	35/70 GB	5 MB/s
DLT8000	40/80 GB	6 MB/s

3.1.7 SuperDLT (SDLT)

SuperDLT (SDLT) is a new format specification designed by Quantum Corporation as an evolution of the DLT standard. It uses Laser Guided Magnetic Recording (LGMR) technology. This technology includes the Pivoting Optical Servo (POS). This optically assisted servo system is implemented on the unused reverse side of the media and uses a laser to read the servo guide. SDLT uses 100% of the media for data recording.

SDLT uses Advanced Metal Powder (AMP) media containing embedded information for the Pivoting Optical Servo system.

The recording mechanism is made of Magneto-Resistive Cluster (MRC) heads, a cluster of small magneto-resistive tape heads.

The first SDLT drive, the SDLT 220, was introduced in late 2000. It provides a capacity of 110 GB (native) and 220 GB (with 2:1 compression). The native data transfer rate is 11 MB/sec. This first drive was not backward-read-compatible with earlier models. In 2001 Quantum released a version of the SDLT 220 drive that was backward-read-compatible with the DLTtape IV cartridge.

Quantum's latest SDLT 320 drive came available in 2002. It increased the native capacity to 160 GB (320 GB with 2:1 compression) and the native transfer rate to 16 MB/sec (32 MB/sec with 2:1 compression). The SDLT 320 is backward read compatible with DLTtape IV cartridges and uses Super DLTtape I media.

10.684
J

3.1.8 IBM 3480

The second generation of IBM magnetic tapes and the first one to use an enclosed cartridge containing 1/2-inch tape, the IBM 3480, was announced on March 22, 1984. The tape was stored in a now-familiar cartridge, which was smaller, much more robust, and easier to handle than tape reels. The cartridge capacity was 200 MB, and the channel data rate was 3 MB/s, writing 18 tracks in one direction.

3.1.9 IBM 3490

The 3490 replaced the 3480 tape technology, using the same tape cartridge media. The IBM 3490E, with a tape capacity of 800 MB uncompacted (2.4 GB compacted) and a channel data rate of 3 MB/s, increased the capacity of the 3480 fourfold by using a double-length tape and by writing data in both directions: 18 tracks to the end of tape, and 18 tracks back to the start of the tape.

During this second generation, several steps were taken to automate tape processing and to reduce or eliminate human intervention. Automatic cartridge loaders and automated tape libraries, such as the StorageTek Silos and the IBM 3495 and 3494 libraries, were introduced to reduce or eliminate the need for tape operators. Software packages, such as CA-1, TLMS, and the DFSMS Removable Media Manager (DFSMSrmm™), were implemented to manage the tape volumes automatically.

The IBM 3490 and compatible drives were probably the first family of tape products that were mostly used with automatic tape libraries rather than being installed as stand-alone drives operated manually.

Applications still used tapes directly, and the Improved Data Recording Capability (IDRC), which compacts the data, reduced the number of tape volumes used.

Magnetic disks were now widely used for online data, and these second-generation tape systems therefore became primarily a medium for backup and were introduced as an archive medium. The process of archiving was also automated with products such as Hierarchical Storage Manager (HSM) and DFSMShsm™ (a component of DFSMS/MVS®) using tape as the lowest level in a storage hierarchy. Of course, tape was still used as an interchange medium, but networks were also used for that purpose.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1292
Doc. 3698

3.1.10 IBM Magstar 3590

IBM Magstar tape technology was first introduced in July 1995. The original cartridge maintained the external form factor of the 3490 (Figure 3-12), had a capacity of 10 GB uncompacted (30 GB compressed), and the data rate was 9 MB/s. Later drive models and new media increased these figures. The data format is not compatible with the 3490.

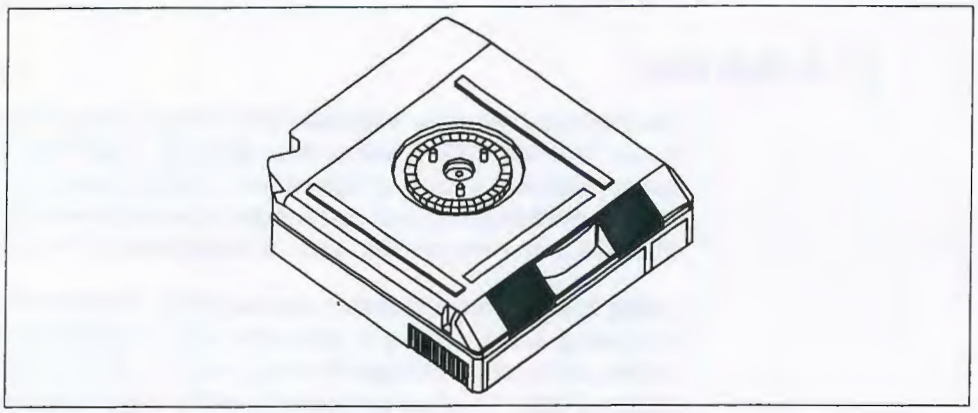


Figure 3-12 Magstar 3590 tape cartridge

The Magstar 3590 drive (see Figure 3-13 on page 65) incorporates a new longitudinal technology, Serpentine Interleaved Longitudinal Recording. Data is written in each direction in turn, and to increase capacity further by providing multiple sets of tracks in parallel, the concept of *head indexing* is introduced. The entire set of heads is slightly shifted after one pass, and all subsequent passes (for a total of eight) are used to write data tracks adjacent to the existing ones. This means a significant improvement in the tape capacity and transfer rates without changing the tape speed (2 m/s) and media length (600 m). A buffer is used, and the data is compressed before it is written to tape. In addition, the drive can complete a stop-start cycle in approximately 100 ms. The performance is significantly improved for both start-stop and streaming applications.

With the IBM TotalStorage Enterprise Magstar 3590 Model H and the Extended Length Cartridges made available in 2002, the capacity and data rate have been increased to 60 GB (180 GB assuming 3:1 compression) and 14 MB/s native respectively, while maintaining backward compatibility for reading with the base models.

10.682

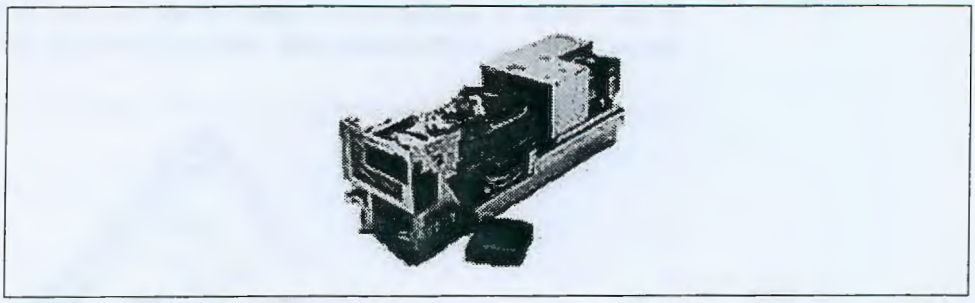


Figure 3-13 Magstar 3590 tape drive

This design incorporates some innovations such as servo tracks on the tape to guide the read/write heads along the data tracks and the implementation of an improved error correcting code (ECC). A portion of the tape within each cartridge is reserved for statistical information; it is continually updated after each read or write, providing statistics that can be used to obtain drive and media information and identify problems with a particular tape or drive as early as possible.

Metal particle media

A chromium dioxide medium was used in the IBM 3480 and 3490 cartridges. The IBM 3590 High Performance Tape Cartridge uses a metal particle medium, which has a significantly increased coercivity and therefore permits a much higher data recording density in comparison with chromium dioxide media. The linear density is proportional to the medium's coercivity, and therefore the linear density of the IBM 3590 tape is approximately three times that of the IBM 3480 and 3490. The track density is also improved approximately fourfold. Advances in the metal particle coatings and media binders afford reliability and magnetic stability equal or superior to chrome media.

3.1.11 STK 9840

Introduced in late 1998, the STK T9840 tape drive (dubbed "Eagle") is based on linear technology and targeted at the high-end, enterprise server market. The dual-hub cartridge (shown in Figure 3-14 on page 66) has a native capacity of 20 GB and a maximum data rate of 10 MB/s. To maintain compatibility with existing enterprise system automation products (mainly the STK silos), the cartridge maintains the external form factor of the 3490/3590 cartridge.

In 2001, StorageTek introduced a second-generation 9840 drive, the T9840B. Tape speed during read/write operations doubled, from 2 m/sec on the T9840A to 4 m/sec on the T9840B, and maximum data transfer rate nearly doubled, to 19 MB/sec. The capacity is still 20 GB (native) and 40 GB (with 2:1 compression).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1293
Doc. 3698

Data on both drives is written 16 tracks at a time in a total of 18 passes, for a total of 288 tracks. In addition to the data tracks, the tape contains five bands of five servo tracks each (25 tracks total) that are pre-written on the tape.

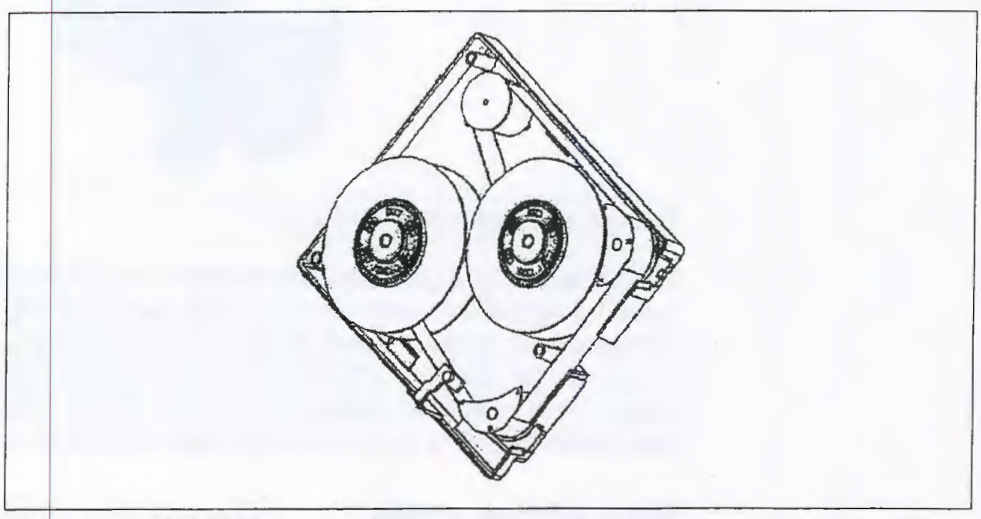


Figure 3-14 STK 9840 tape cartridge

3.1.12 STK 9940

The STK T9940 is based on T9840 technology. The biggest differences between these two drives are the data cartridge and the loader mechanism for the cartridge. TheT9940 cartridge has the same form factor and dimensions as the T9840 cartridge, but the T9940 cartridge contains a single reel of media, and the tape path, take-up reel, and tape guidance system are located inside the drive. The first-generation T9940A drive has a capacity of 60 GB (native) and 120 GB (with 2:1 compression). The native data transfer rate is 10 MB/sec.

The StorageTek T9940B format, made available at the end of 2002, increased the capacity and data transfer rate of the prior generation to 200 GB (400 GB with 2:1 compression) and 30 MB/s native. the T9940B drive is backward-read-compatible with the T9940A model.

3.1.13 LTO Ultrium

The Linear Tape-Open (LTO) standard was released as a joint initiative of IBM, Hewlett-Packard, and Seagate Companies. As result of this initiative, two LTO formats (Ultrium and Accelis) were defined.

10.680
J

The consortium of these companies is known as the Technology Provider Companies. The new technology specifications are detailed at an LTO Web site:

`http://www.lto-technology.com`

The IBM LTO Ultrium 1 drive provides a single-media capacity of up to 100 GB (200 GB with 2:1 compression) data storage per cartridge and a sustained data rate of up to 15 MBps (uncompressed), while the newly released IBM LTO Ultrium 2 drive has doubled media capacity to 200 GB (400 GB with 2:1 compression) data storage per cartridge and more than doubled sustained data rate to 35 MBps (uncompressed).

For a detailed description of the LTO Ultrium tape format specification, see 1.2.2, "LTO core technology" on page 6.

For a detailed description of the IBM LTO Ultrium drive, see 2.4, "IBM LTO Ultrium common subassembly" on page 28.

3.1.14 Libraries

System administrators are clamoring for technologies that enable them to efficiently and economically manage the explosive growth in stored data. As the amount of data increases, the backup process takes longer and longer.

The solution to this problem is to use a device that integrates the tape drive with some level of automation. The challenge is to choose the right solution in terms of size and automation level.

System administrators industry-wide have recognized the need for automating the backup-and-restore process to the extent that little or no human intervention is required. This has come to be known as *lights-out backup*. This process can be done off-shift, or concurrently with other applications during normal operations. Multi-drive tape libraries are the only available technology that offer both the reliability and low cost to make lights-out backup practical.

The hardware options for automation are autoloaders and a range of multi-drive automated tape libraries. We distinguish between them below.

Autoloaders

Autoloaders have one tape drive and typically are used to access a small number of tapes once a day. Most are designed for purely sequential operations. These units place no emphasis on performance.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1294
Doc. 3698

Automated tape libraries

Automated tape libraries have one or more tape drives, but typically are used with at least two tape drives. All tape cartridges are accessible to all drives, thus making concurrent reading and writing operations possible.

Throughput can be increased by adding additional drives. Libraries can exchange tapes in a few seconds, substantially improving file-restore response times. Tape libraries are mandatory for lights-out operations and other higher performance tape storage applications. Tape libraries also offer the security of knowing that other drives will take over if one should fail.

Multi-drive automated tape libraries and ultra-scalable tape libraries combined with storage-management software, including concurrent backup, archive, and HSM, offers the most robust solution to manage and protect huge amounts of corporate data. Automated tape libraries allow random access to large numbers of tape cartridges and concurrent use of two or more drives, rather than manually loading one tape after another or using a single-drive sequential autoloader.

Enterprise tape libraries

Enterprise tape libraries are automated tape libraries that provide enhanced levels of automation, scalability, reliability, availability and serviceability. They typically have the capacity to house dozens of drives and hundreds of tapes. Equipped with high-performance robotic mechanisms, bar code scanners, and support for cartridge I/O ports, these libraries often offer redundant components and a high degree of flexibility through a modular design. Some models add support for multiple SCSI, FC-AL, FCP, and ESCON®, or FICON™ connections to allow connection to more than one host platform. At the top of the line of the enterprise tape libraries are products such as the IBM TotalStorage Enterprise Tape Library 3494 and the IBM TotalStorage UltraScalable Tape Library 3584 that are designed to be shared between two or more heterogeneous host systems. All the hosts have access to the control functions of the tape library robotics. Simply put, the library is shared in a physical way, with each system thinking it really owns the entire library.

3.2 Current SAN technologies

A SAN (Storage Area Network) is a high-speed network that enables the establishment of direct connections between storage devices and processors (servers) within the distance supported by Fibre Channel.The SAN can be viewed as an extension to the storage bus concept that enables storage devices and servers to be interconnected using elements similar to Local Area Networks (LANs) and Wide Area Networks (WANs): routers, hubs, switches, directors, and

10678
A

gateways. A SAN can be shared between servers or dedicated to one server. It can be local or extended over geographical distances.

In today's SAN environment the storage devices in the bottom tier are centralized and interconnected, which represents, in effect, a move back to the central storage model of the host or mainframe.

Figure 3-15 shows a tiered overview of a SAN connecting multiple servers to multiple storage systems.

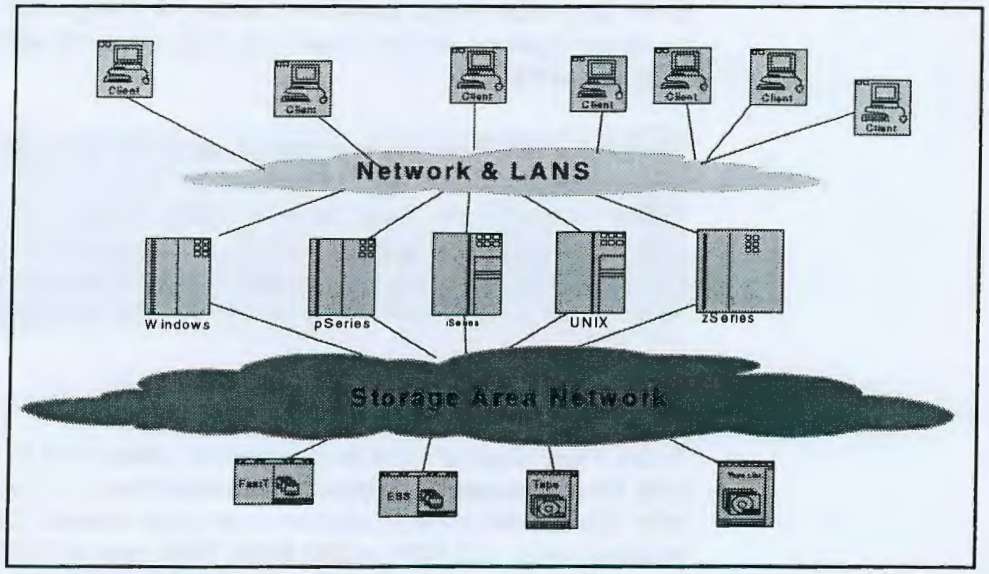


Figure 3-15 Overview of a SAN

A SAN facilitates direct, high-speed data transfers between servers and storage devices, potentially in any of the following three ways:

- Server to storage: This is the traditional model of interaction with storage devices. The advantage is that the same storage device may be accessed serially or concurrently by multiple servers.
- Server to server: A SAN may be used for high-speed, high-volume communications between servers.
- Storage to storage: This outboard data movement capability enables data to be moved without server intervention, thereby freeing up server processor cycles for other activities such as application processing. Examples include a disk device backing up its data to a tape device without server intervention, or a remote device mirroring across the SAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1295
Doc 3698

3.2.1 SAN definition

The Storage Network Industry Association (SNIA) defines SAN as a network whose primary purpose is the transfer of data between computer systems and storage elements and among storage elements. A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage elements, and computer systems so that data transfer is secure and robust. The term SAN is usually (but not necessarily) identified with block I/O services rather than file access services.

It can also be a storage system consisting of storage elements, storage devices, computer systems, and/or appliances, plus all control software, communicating over a network.

Note: The SNIA definition specifically does not identify the term SAN with Fibre Channel technology. When the term SAN is used in connection with Fibre Channel technology, use of a qualified phrase such as *Fibre Channel SAN* is encouraged. According to this definition, an Ethernet-based network whose primary purpose is to provide access to storage elements would be considered a SAN. SANs are also used for system interconnection in clusters.

3.2.2 Fibre Channel architecture

Today, Fibre Channel is the architecture on which most SAN implementations are built. Fibre Channel is a technology standard that enables data to be transferred from one network node to another at very high speeds. Current implementations transfer data at 100 MB/s or 200 MB/s. Data rates of 1000 MB/s have been tested and many companies have products in development that will support this. The Fibre Channel standard is accredited by many standards bodies, technical associations, vendors, and industry-wide consortia. There are many products on the market that take advantage of its high-speed, high-availability characteristics.

Fibre Channel was completely developed through industry cooperation, unlike SCSI, which was developed by a vendor and submitted for standardization after the fact.

Note: The word *Fibre* in Fibre Channel is spelled in the French way rather than the American way because the interconnections between nodes are not necessarily based on fiber optics, but could be based on copper cables. It is also the ANSI X3T11 technical committee's preferred spelling. This is the standards organization responsible for Fibre Channel and certain other standards for moving electronic data in and out of computers. Even though copper-cable-based SANs are rare, the spelling has remained.

10676
A.

3.2.3 Topologies

Fibre Channel interconnects nodes using three physical topologies that can themselves have variants. These topologies are:

- Point-to-point: The point-to-point topology consists of a single connection between two nodes. All of the bandwidth is dedicated for these two nodes.
- Loop: In the loop topology, the bandwidth is shared between all the nodes connected to the loop. The loop can be wired node-to-node; however, if a node fails or is not powered on, the loop is out of operation. This is overcome by using a hub. A hub opens the loop when a new node is connected and closes it when a node disconnects. A major drawback in this technology is the Loop Initialization Process (LIP), which needs to occur every time a node is removed from the loop or a new node is added to the loop. The LIP process disrupts the loop and can cause data disruptions.
- Switched: A switch enables multiple concurrent connections between nodes. This is generally referred to as a switched fabric. Switched fabric is more reliable than a loop because there is no need for the LIP process. New nodes can be added and removed without any disruption to the Fibre Channel processes.

3.2.4 Tape solutions in a SAN environment

Connectivity to tape is essential for most backup processes. However, manual tape operations and tape handling are expensive. Studies show that automation of tape processing saves money and increases reliability. Enterprises have long had to utilize staff to remove these tapes, transport them to a storage site, and then return them to the tape drive for mounting when needed. Customer tape planning initiatives are directed at more efficient utilization of drives and libraries, as well as minimization of manual labor associated with tape processing.

The biggest issues with SCSI tape implementations are the limited cable length and the limited possibilities to share drives between several systems. For LVD SCSI the total cable length is limited to 25 m using point-to-point interconnection (such as one host connected to only one tape drive). With multi-drop interconnection (one host connected to more than one tape drive on the same SCSI bus) the total cable length is 12 m for LVD SCSI and 25 m for HVD SCSI. Most SCSI tape drives currently have only one SCSI port and hence can only be attached on one SCSI bus. This severely limits the number of hosts that can physically allocate the drive without recabling.

SANs enable greater connectivity of the tape libraries and tape drives, as well as tape sharing, which will be discussed later in this chapter. With Fibre Channel the distance between the server (or data point) and the connected tape node can be up to 10 km. Fibre Channel enables multiple host scenarios without recabling.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1296
Doc. 3698

If software to manage tape-drive sharing is not available, we would have to isolate (or *zone*) the drives to unique hosts using functions commonly available on SAN gateways or switches. With the proper management software, each drive can talk to each host, and connections can be dynamic without recabling.

Backup solutions can utilize SAN technology in a number of ways to reduce the costs of their implementation and at the same time increase their performance.

Sharing tape devices on a SAN environment

The tape world has three distinct means of sharing:

- Library sharing
- Drive sharing
- Media sharing

Library sharing

Library sharing occurs when multiple servers attached to a tape library share both the library and the robotics. The tape drives within the library may or may not be shared (pooled) among the attached servers. Tape library sharing is a prerequisite for tape-drive sharing.

Drive sharing

The sharing of one or more tape drives between multiple servers is called drive sharing. To share drives between heterogeneous applications within a tape library, the tape library must provide multiple paths to the robotics and also must have the capability to define the library's drives and slots as multiple logical libraries. The server attached to each partition has no knowledge of any drives or slots outside the partition.

Media sharing

Media sharing today is only possible in a homogeneous environment between servers that use the same backup server and the same library to back up their data. For systems that are not backed up by the same backup server it is only possible to share a tape scratch pool.

Figure 3-16 on page 73 shows the multi-path architecture of the 3584 LTO tape library. Every drive can have a path defined to the SCSI Medium Changer (SMC).

The library on the left has been partitioned into three logical libraries. In the AIX and NT partitions, only the first drive has a library control path defined.

The iSeries is unique in that every IOP/IAP has to have a library control path defined. The iSeries attached to the left-hand library has two SCSI buses and therefore, two library control paths defined. These three servers are sharing the 3584 LTO tape library but not the drives.

The library on the right has not been partitioned, and has only one logical library. Every iSeries SCSI bus has a library control path defined to allow control of the 3584 robotics. The iSeries supports the attachment of one Ultrium 1 LTO tape drive and of up to 15 Ultrium 2 LTO tape drives per SCSI bus.

The iSeries Servers attached to the right-hand library are also sharing the library even thoughit has not been partitioned. Through BRMS the iSeries Servers are sharing the library and media, but no tape-drive pooling is being done.

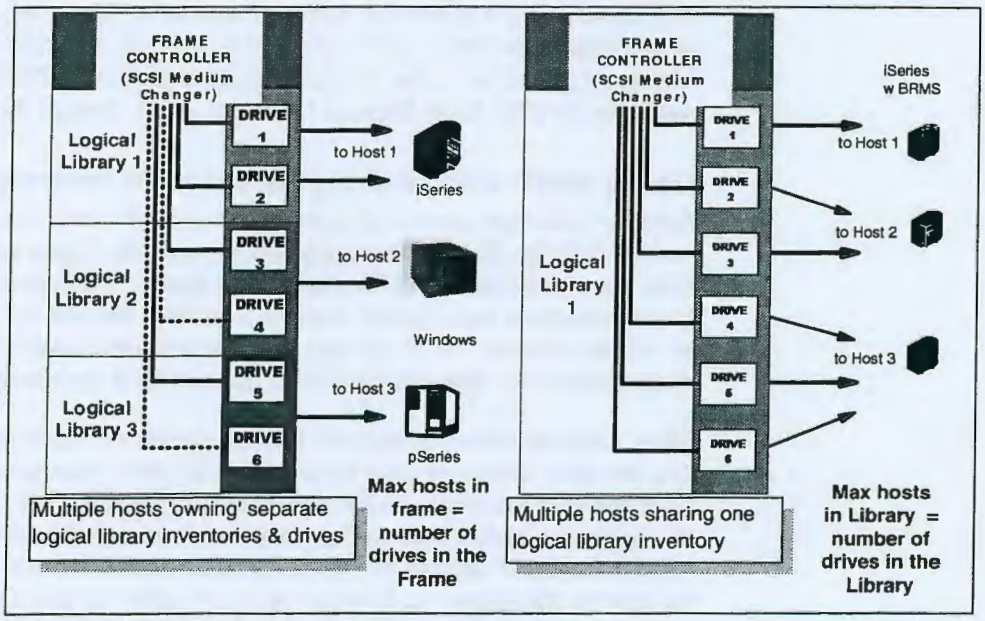


Figure 3-16 IBM 3584 multi-path architecture

IBM LTO in SAN environment

The new IBM LTO Ultrium 2 Tape Drives are available with a Fibre Channel interface for either point-to-point or Fibre Channel-Arbitrated Loop attachment. These options remove the need to use a SAN data gateway. The device can be attached directly to SAN switches or FC-AL hubs.

For IBM LTO Ultrium 1 Tape Drives, SAN attachment must occur via a SAN data gateway. For drives with LVD interfaces, attachment must be through the SAN Data Gateway Router, 2108-R03. For drives with HVD interfaces, attachment must be through either the SAN Data Gateway Router, 2108-R03, or the SAN Data Gateway for Tape, 2108-G07.

In each case, the server will require a supported Fibre Channel HBA.

ROS nº 03/2005 CN
CPMI - CORREIOS
Fls. Nº 1297
Doc. 3698

Backup software for SAN environments

Implementing backup solutions in a SAN topology requires software developed to enable the sharing of tape drives at a logical level. The major benefits of this software are:

- Direct connection of the tape drive to the server for high speed
- Sharing the drive with another server to save money

All you need is the proper traffic control feature at a software level.

The development of backup software solutions supporting tape-sharing on SAN is an ongoing process, and many of the back-up software vendors have already delivered products or plan to deliver such a product. IBM has made tape-sharing available for IBM Tivoli Storage Manager since Version 3.7 (October 1999).

Using electronic vaulting for disaster recovery

Another important aspect of using tape in a SAN is the opportunity to exploit tape connectivity for disaster recovery enhancements. Today most enterprises take their tape backups offsite for disaster recovery. The tape is actually created in a locally attached tape library, then ejected from the library, and finally removed to an offsite location. All of this requires manual intervention and is error-prone. A major reason for failed recoveries is caused by a tape being mis-placed.

Fibre Channel SANs enable the backup server to create tapes easily and safely in a remotely attached tape library. This is called electronic vaulting. It removes all of the manual effort, as the tape is already offsite, and prevents a major cause of disaster-recovery failure. Currently, most enterprises staff tape operations to handle the tapes as they come and go from offsite storage. Fibre Channel allows for greater distances, so it becomes much easier to put a remote tape library at another location to create the backup tape copy. With this method, outlined in Figure 3-17 on page 75, no manual handling is necessary.

10674
A.

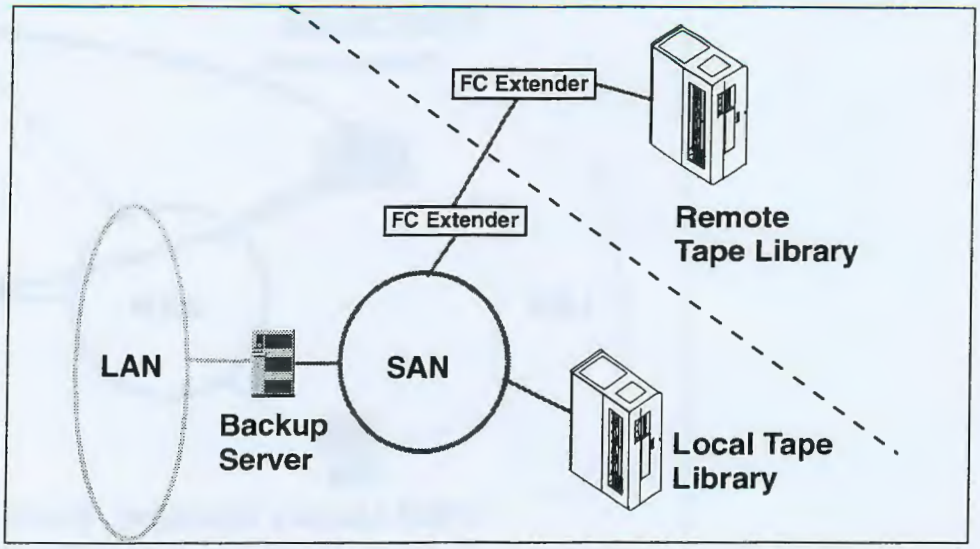


Figure 3-17 Electronic vaulting

LAN-free backup

SAN technology provides an alternative path for data movement between the backup client and the server. Shared storage resources (disk, tape) are accessible to both the client and the server through the SAN. Data movement is off-loaded from the LAN and from the server processor and allows for greater scalability. LAN-free backups decrease the load on the LAN.

Managed System for SAN is a feature of IBM Tivoli Storage Manager that enables LAN-free data movement. The Tivoli Storage Manager client data moves directly to and from a storage device attached to a SAN. A Tivoli Storage Manager storage agent is installed on the client machine and shares storage resources with the Tivoli Storage Manager server. The storage agent can write directly to storage media in a format that is consistent with that used by the server. The Tivoli Storage Manager server or servers controls the storage devices and keeps track of the data that the client has stored. Tivoli Storage Manager continues to use a LAN connection to exchange control information, such as policy information and data about the objects that are backed up. Using the SAN for client data movement decreases the load on the Tivoli Storage Manager server and allows the server to support a greater number of simultaneous client connections. See Figure 3-18 on page 76.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1298
Doc. 3698

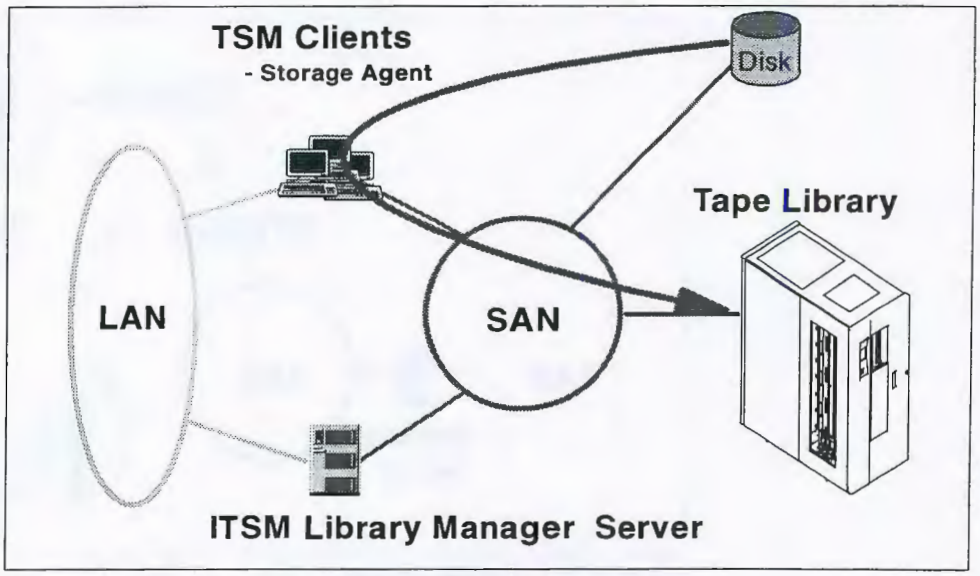


Figure 3-18 Tivoli Storage Manager LAN-free backup

The storage agent communicates with the server via the LAN to obtain and store database information and to coordinate device and volume access. The server determines if the client is requesting access to storage for which the client has a SAN path defined. If a SAN path is defined, the client (by means of the storage agent) transfers data on that path. If a failure occurs on the SAN path, failover occurs and the client uses its LAN connection to the Tivoli Storage Manager server and moves the client data over the LAN.

Server-free backup

Server-free data movement provides a way to back up and restore large volumes of data between client-owned disks and storage devices in a method that reduces overhead on the backup server and the backup client, and that minimizes data transfer on the LAN. This is done by making use of the SCSI–3 extended copy command. The command is issued and initiated by the server and carried out by a data mover device (e.g. SAN Data Gateway) that exists on the SAN. The data mover device is responsible for moving the data either from a SAN-attached client-owned disk to a SAN-attached tape drive, or from a SAN-attached tape drive to a SAN-attached client-owned disk, which frees the server and the client from the operation. The process is shown in Figure 3-19 on page 77.

Server-free backup/restore capability was introduced into IBM Tivoli Storage Manager in Version 5 for certain platforms. For more information on server-free capabilities of Tivoli Storage Manager, see the support page at `http://www-3.ibm.com/software/tivoli/products/storage-mgr-san/platforms.html` and the redbook *IBM Tivoli Storage Manager Version 5.1 Technical Guide*, SG24-6554.

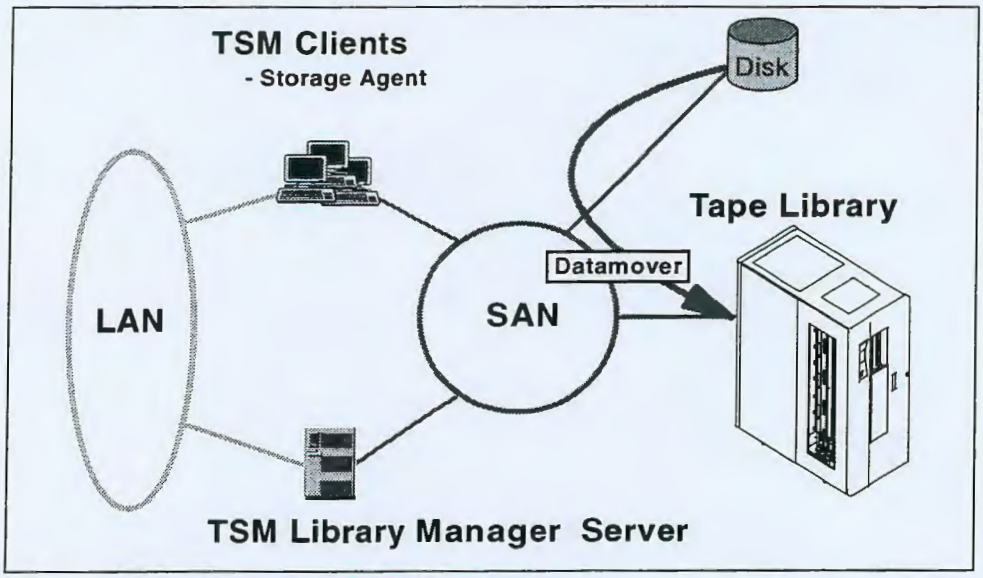


Figure 3-19 Tivoli Storage Manager server-free backup

RQS nº 03/2005 - CN
CPMI - CORREIOS
1299
Fls. Nº
Doc. 3698

10671
A

4

IBM TotalStorage Ultrium Tape Drive 3580

The IBM TotalStorage Ultrium Tape Drive 3580 is the smallest in the family of IBM Ultrium tape solutions. It is an external, stand-alone, SCSI-attached tape drive that attaches to iSeries, pSeries, xSeries, RS/6000® SP, and other UNIX and PC servers supporting OS/400®, IBM AIX, Sun Solaris™, HP-UX, Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows 2003, and Red Hat and SuSE Linux using a suitable SCSI adapter.

The IBM 3580 Ultrium tape drive is a very cost-effective solution for save-and-restore and archiving functions, and it provides an excellent migration path from SDLT, 1/4-inch, 4 mm, or 8 mm tape drives.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 CN
CPMI CORREIOS
FIS. Nº 1300
3698
Doc.

4.1 Model description

The IBM 3580 is a large-capacity, high-performance Ultrium tape drive available as six separate model types, depending on the capacity and SCSI[1] interface required.

Figure 4-1 IBM 3580 model L11/L13/L23 or H11/H13/H23 Ultrium tape drive

There are six model types:

- *IBM 3580-L11* and *IBM 3580-L13* have 100GB native capacity with a Low-Voltage Differential (LVD) Ultra2 SCSI attachment that connects to LVD fast/wide adapters.
- *IBM 3580-H11* and *IBM 3580-H13* have 100GB native capacity with a High-Voltage Differential (HVD) Ultra SCSI attachment that connects to HVD fast/wide adapters.
- *IBM 3580-L23* has 200GB native capacity with a Low-Voltage Differential (LVD) Ultra2 SCSI attachment that connects to LVD fast/wide adapters.
- *IBM 3580-H23* has 200GB native capacity with a High-Voltage Differential (HVD) Ultra SCSI attachment that connects to HVD fast/wide adapters.

The IBM 3580 models L11, L13, H11, and H13 all use the Ultrium 1 LTO cartridge, which has a capacity of 100GB (200GB with 2:1 compression), and are capable of sustaining a data rate of up to 15 MB/s (uncompressed).

[1] Refer to 2.4.3, "Interfaces" on page 31 for an explanation of HVD and LVD.

10669
A.

The IBM 3580-L11 and IBM 3580-L13 are functionally identical. The only difference is that the IBM 3580-L13 has a three-year Customer Element Exchange warranty. The IBM 3580-H11 and IBM 3580-H13 are functionally identical; the only difference is that the IBM 3580-H13 has a three-year Customer Element Exchange warranty.

The IBM 3580-L23 and H23 use the Ultrium 2 LTO cartridge, which has a capacity of 200GB (400GB with 2:1 compression), and are capable of sustaining a data rate of up to 35 MB/s (uncompressed).

Note: Although the IBM 3580 Ultrium tape drive provides the capability for high tape performance, other components of the system may limit the actual performance achieved. Also, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

4.2 Feature codes

The IBM 3580 Ultrium tape drive can be ordered with the following feature codes (Table 4-1). We have not included the various cabling options; refer to the product publications for detailed information about configuring and ordering it.

Table 4-1 IBM 3580 feature codes

Feature code	Description	Comments
1748	Custom QuickShip	
8001	One 100GB data cartridge	Plant only; see Media section for details.
8101	One 200GB data cartridge	Plant only; see Media section for details.
8002	One cleaning cartridge	Plant only; see Media section for details.
8723	Rack mount kit	
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9215	Attached to Linux	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1301
Doc. 3698

Feature code	Description	Comments
9400	Attached to AS/400®	
9600	Attached to AIX	

4.3 SCSI attachment

The SCSI interface (HVD or LVD) on each IBM 3580 Ultrium tape drive is chosen by selecting the appropriate model number (model H11/13/23 or L11/L13/23).

The IBM 3580 Ultrium tape drive can be attached to IBM pSeries, IBM xSeries, IBM RS/6000 SP systems, IBM iSeries, AS/400, and non-IBM servers, workstations, and personal computers that support Ultra/Wide SCSI HVD and Ultra2/Wide SCSI LVD interface specifications. The interface you choose will depend on the available adapter in the host, which must be of the same type as the drive interface.

The IBM 3580 Ultrium tape drive also may be compatible with other servers, operating systems, and SCSI adapters. Contact your local IBM representative for a current list of supported open system configuration and software vendors or visit `http://www.ibm.com/storage/lto`.

4.4 SCSI cabling

A SCSI cable is required for each IBM 3580 connection to a SCSI bus. A single 2.5 m SCSI cable is available as a no-charge feature; if an alternate length is required it should be included in the initial order. A SCSI terminator is included with each drive.

An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) also may be required for attachment to particular server adapters.

4.4.1 Cables

A single SCSI cable is available as a no-charge feature (either #9702 or #9703) specified only with the initial IBM 3580 order. It is not orderable as a miscellaneous equipment specification (MES) for installation later. Feature #9702 supplies a 2.5 m universal SCSI cable with HD68 connectors at each end; feature #9703 supplies a VHDCI connector at one end and HD68 at the other.

10667
A.

Additional SCSI cables are available as optional features on the IBM 3580 for LVD and HVD attachment to host adapters.

The following cables have an HD68 connector at each end:

- Feature #5301, 0.4 m (1.4 feet) SCSI cable
- Feature #5302, 2.5 m (6.6 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The following cables have a VHDCI connector at one end and an HD68 connector at the other end:

- Feature #5602, 2.5 m (6.6 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 25 m (82 feet) SCSI cable

4.4.2 Interposers

An interposer may be required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries adapter #6501.
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable. The interposer (a 0.3 m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

4.4.3 SCSI length limitations

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection. If using multi-drop interconnection, then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using point-to-point or multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1302
Doc. 3698

4.5 Upgrades

The IBM 3580-L11/L13 and IBM 3580-H11/H13 cannot be upgraded to IBM 3580-L23 and IBM 3580-H23, respectively.

IBM 3580 drives cannot be installed into IBM 3581, 3582, 3583, or 3584 units.

4.6 Environmental specifications

The IBM 3580 is designed to be placed on or beside the attached host server or installed in a standard 19-inch rack.

4.6.1 Physical dimensions

The IBM 3580 is a relatively small single tape drive enclosure:

- Width: 17.1 cm (6.75 in)
- Depth: 33.3 cm (13.1 in)
- Height: 14.6 cm (5.75 in)
- Maximum weight: 6.6 kg (14.3 lbs)

4.6.2 Operating environment

The IBM 3580 can be installed in a normal office environment and does not need to be in a specialized machine room. Refer to the product publications for specific information.

4.7 Host platforms and device drivers

The following no-charge specify codes indicate the server platform to which the IBM 3580 Ultrium tape drive is attached:

- #9210, attached to HP-UX
- #9211, attached to Sun System
- #9212, attached to Windows NT or Windows 2000 System
- #9213, attached to other non-IBM system
- #9215, attached to Linux system
- #9400, attached to AS/400 System
- #9600, attached to RS/6000

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3580). Sometimes the driver code is supplied as part of the operating system code (for example, in

10665
A.

OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

Ultrium 1

The IBM 3580 is shipped with device drivers to support Ultrium 1 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.2 or later
- Sun Solaris 2.6, 7, and 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- HP-UX 11.0
- OS/400 V4R4

Ultrium 2

The IBM 3580 is shipped with device drivers to support Ultrium 2 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.3, 5.1
- Sun Solaris 7, 8, and 9
- Windows NT 4.0 with Service Pack 6
- Windows 2000 (build 2195)
- Windows 2003
- HP-UX 11.0, 11i
- OS/400 V5R1, V5R2
- Linux Red Hat 7.2 (32 and 64 bit kernels), Red Hat 7.3, Red Hat Advanced Server 2.1, SuSE Linux Enterprise Server Update

Tip: The device driver CD or diskette that is shipped with the IBM 3580 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

4.7.1 Device driver installation

Install the IBM device drivers for the IBM 3580 as follows:

- If you intend to use the IBM 3580 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3580.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1303
Doc 3698

- If you do not intend to use the IBM 3580 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide* GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3580 with a commercial software application, IBM recommends that you install any IBM supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples of using the Ultrium drives are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

4.8 Storage applications

The software to manage the IBM 3580 Ultrium tape drive is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software providers. A list of compatible software is available at the Web site:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium support and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more detailed information of specific versions and platforms supported.

4.9 Performance considerations

For best performance, it is recommended to attach only one tape drive per SCSI bus. This may not be a realistic objective, but minimizing the number of devices per bus will improve performance. Attaching other SCSI devices on the same SCSI bus as the IBM 3580 Ultrium tape drive may affect performance of those devices.

iSeries configurators allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape drive on an input/output port may affect system performance.

10663
A.

Although the compression technology can increase the amount of data stored on the media, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

4.10 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each IBM 3580 drive order[2]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3580:

- Feature #8001 provides a single 100 MB Ultrium 1 Data Cartridge. It is a chargeable feature, and a maximum of five can be ordered.
- Feature #8101 provides a single 200 MB Ultrium 2 Data Cartridge. Additional cartridges can be ordered using part number #08L9870.
- Feature #8002 provides a single Ultrium Cleaning Cartridge. It is a chargeable feature, and a maximum of three can be ordered.

Subsequent to the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about how to order supplies and cartridges, with or without labels.

4.11 IBM 3580 Ultrium tape drive initial set-up

This section covers some of the major items required to implement, manage, and operate the IBM 3580 tape drives. It does not cover all of the tasks, nor do we intend to cover all the specific commands. For more details, refer to *IBM 3580 Ultrium Tape Drive Setup, Operator and Service Guide*, GA32-0415, *IBM TotalStorage LTO Ultrium 2 Tape Drive 3580 Setup and Operator Guide*, GA32-0460, and the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268 and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

4.11.1 SCSI ID

If you attach multiple IBM 3580 SCSI devices in the same chain, they should each use different SCSI IDs starting with the lowest number on the first device as depicted in Figure 4-2 on page 88. The last device of that SCSI chain must have a valid terminator. The SCSI ID set-up button is located at the rear of the IBM 3580.

[2] All media and cleaning cartridges are warranted separately from the IBM 3580 Ultrium tape drive.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1304
Doc. 3698

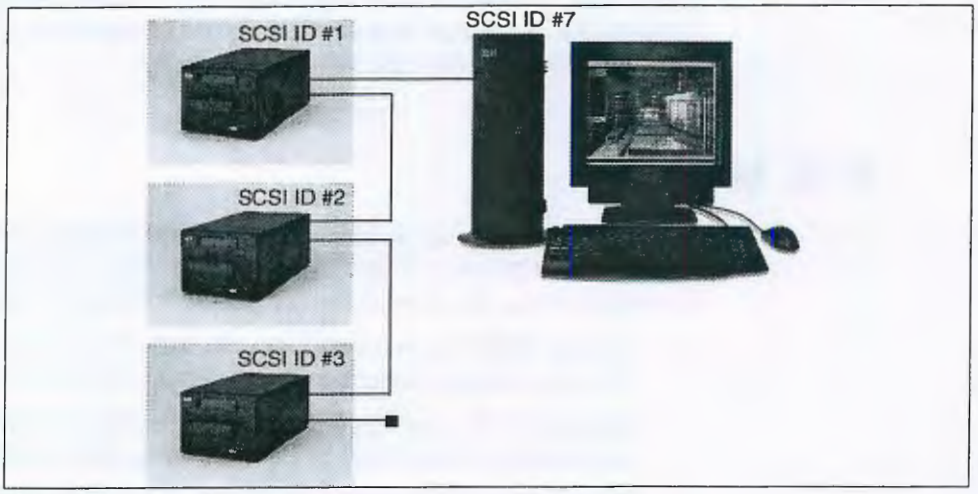


Figure 4-2 SCSI ID set-up example

4.12 Operator displays and buttons

The IBM 3580 Ultrium tape drive has a simple operating interface consisting of:

- A status light
- A message display
- A single character display
- A push button

4.12.1 Status light

The status light (labeled 2 in Figure 4-3 on page 90) provides information about the state of the IBM 3580 tape drive. The light can be green or amber, and, when lit, solid or flashing. These are the possible conditions of the status light and an explanation of what each condition means:

- Off: The IBM 3580 tape drive has no power, or is powered off, or if C displays simultaneously in the single-character display (see label 3 in Figure 4-3 on page 90), it needs cleaning.
- Green/solid: The IBM 3580 tape drive is idle.
- Green/flashing: The IBM 3580 tape drive is reading or writing data, rewinding the tape, locating data on the tape, or unloading the tape.
- Yellow/solid: The IBM 3580 tape drive is in maintenance mode, or is running power-on self-test diagnostic routines.

- Yellow/flashing: One of the following applies:
  - If the light flashes once per second, an error occurred and the tape drive or media may require service. Note the code on the single-character display. Refer to the Setup and Operator Guides (GA32-0415 for Ultrium1 or GA32-0460 for Ultrium 2).
  - If the light flashes twice per second, the tape drive is updating firmware.
  - If the light flashes four times per second, the tape drive detected an error and is performing a firmware recovery. It resets automatically.

4.12.2 Message display

The message display (labeled 4 in Figure 4-3 on page 90) is a liquid crystal display (LCD) that provides information about the status of the tape drive and error conditions.

The message display consists of two rows, with 20 characters available in each row. During operation, the IBM 3580 tape drive continuously queries the drive and updates the display with status messages. When in an idle (non-operating) state, the tape drive displays the following messages:

```
Ultrium Tape Drive
Drive Empty
```

4.12.3 The single-character display

The IBM 3580 tape drive features a light-emitting diode (LED) display (labeled 3 in Figure 4-3 on page 90 below). The LED presents a single-character code for:

- Error conditions and informational messages
- Diagnostic or maintenance functions (while in maintenance mode only)

For the list of messages, refer to the Setup and Operator Guides (GA32-0415 for Ultrium1 or GA32-0460 for Ultrium 2).

If multiple errors occur, the code with the highest priority (represented by the lowest number) displays first. When the error is corrected, the code with the next highest priority displays, and so on, until no errors remain.

The single-character display is blank during normal operation of the IBM 3580 tape drive.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1305
3698
Doc

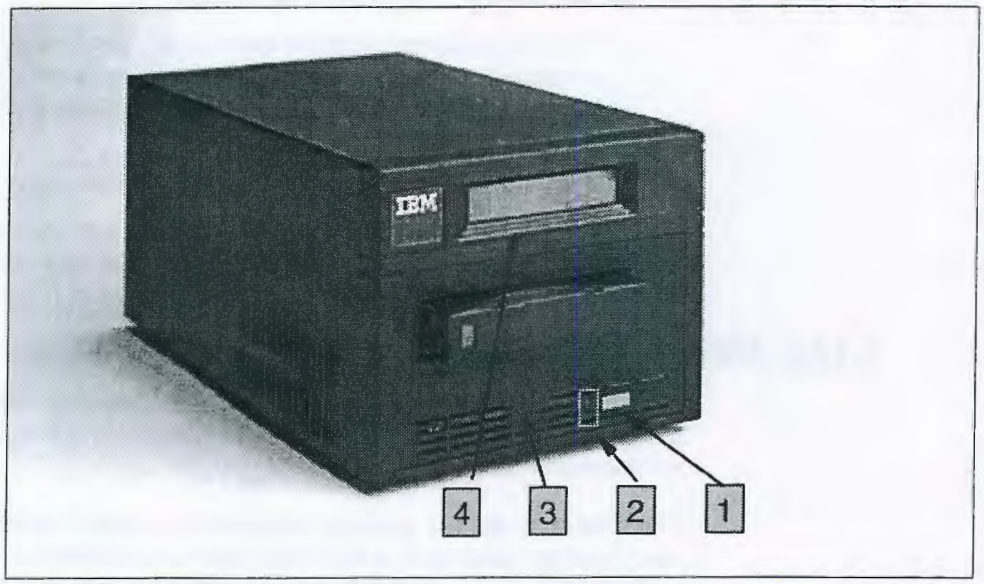


Figure 4-3 Front view of the IBM 3580 tape drive

4.12.4 Unload push button

The unload push button (labeled 1 in Figure 4-3) enables you to perform several functions. You can:

- Rewind the tape from the cartridge and eject the cartridge from the tape drive.
- Place the tape drive in maintenance mode
- Scroll through the maintenance menus
- Exit from the maintenance mode.

Attention: If you press the Unload button during operation, the IBM 3580 tape drive ends the current job, and unloads and ejects the tape cartridge.

4.13 Drive cleaning

All IBM Ultrium tape drives have an integrated cleaning mechanism that brushes the head at cartridge load time and again when unloading a cartridge. Along with this, the drives have a cleaning procedure that uses a special cleaning cartridge.

To clean the head, insert the cleaning cartridge into the tape load compartment. The tape drive performs the cleaning operation automatically. When the cleaning operation is finished, the drive ejects the cartridge.

10659
A-

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

The IBM 3580 needs cleaning when the IBM 3580 tape drive status light (label 2 in Figure 4-3 on page 90) is OFF and C displays simultaneously in the single-character display (label 3 in Figure 4-3 on page 90). This is the only occasion when a cleaning cartridge should be used. For normal operation, the integrated cleaning mechanism ensures that the head remains clean.

4.14 Firmware upgrade

Each IBM Ultrium Tape drive contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the latest firmware level is installed on your IBM LTO tape drive. As the IBM 3580 is designated as a Customer Setup Machine, it is the customer's responsibility to have current firmware installed.

Determine the latest level of firmware available from the Web site:

`http://www-1.ibm.com/support/docview.wss?rs=543&org=ssg&doc=S4000055&loc=en-us`

Follow the instructions for updating your firmware in the Setup and Operator Guides (GA32-0415 for Ultrium1 or GA32-0460 for Ultrium 2) or from:

`http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_drivefw`

RQS nº 03/2005 CN
CPMI - CORREIOS
Nº 1306
3698
Doc.

10658

5

IBM TotalStorage Ultrium Tape Autoloader 3581

The IBM TotalStorage Ultrium Tape Autoloader 3581 (see Figure 5-1 on page 95) is the second product in the IBM LTO Ultrium family. It is an external, single-drive, SCSI-attached, stand-alone or rack-mounted autoloader that attaches to iSeries, AS/400, pSeries, RS/6000, RS/6000 SP, xSeries, Netfinity®,Microsoft Windows NT, Microsoft Windows 2000, Windows 2003, Sun Solaris, HP-UX, and Linux systems using a SCSI adapter.

The IBM TotalStorage Ultrium Tape Autoloader 3581 uses a single IBM LTO Ultrium tape drive. The autoloader contains seven tape slots[1] providing a media capacity of up to 700 GB (1.4 TB with 2:1 compression) per autoloader, and is capable of sustaining a data rate of up to 15 MBps (uncompressed).

The IBM TotalStorage Ultrium Tape Autoloader 3581 is an excellent solution for customers who use tape and require a larger capacity or higher performance tape backup, with or without random access, than is provided by their current tape system. With its higher capacity and performance, the 3581 is an excellent replacement for other externally attached DLT, SDLT, 1/4-inch, 4 mm, or 8 mm tape devices for the iSeries, AS/400, pSeries, RS/6000, RS/6000 SP, xSeries, and Netfinity families of workstations and servers.

[1] When the optional barcode reader is installed the cartridge capacity is reduced to six.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1307
3698
Doc.

For capacity and performance requirements beyond a single IBM Ultrium drive and seven IBM Ultrium tape cartridges, consider other solutions in the IBM Ultrium familysuch as the IBM TotalStorage Tape Library 3582, IBM TotalStorage Ultrium Scalable Tape Library 3583, or IBM TotalStorage UltraScalable Tape Library 3584.

10656
CA

5.1 Model description

The IBM TotalStorage Ultrium Tape Autoloader 3581 is a high-performance Ultrium tape autoloader. It is available as four separate model types, depending on the capacity and required SCSI[2] interface.

Figure 5-1 IBM TotalStorage Ultrium Tape Autoloader 3581

The four models are:

- *IBM 3581-L17* and *IBM 3581-L13* have seven cartridge slots, a .7 TB native data capacity with a Low-Voltage Differential (LVD) Ultra2 SCSI attachment that connects to LVD fast/wide adapters.
- *IBM 3581-H17* and *IBM 3581-L13* have seven cartridge slots, a .7 TB native data capacity with a High-Voltage Differential (HVD) Ultra SCSI attachment that connects to HVD fast/wide adapters.

The IBM 3581-L17, -L13, -H17, and -H13 all use the same Ultrium 1 LTO cartridge, which has a capacity of 100GB (200GB with 2:1 compression), and are capable of sustaining a data rate of up to 15 MB/s (uncompressed).

[2] Refer to2.4.3, "Interfaces" on page 31 for an explanation of HVD and LVD.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1308
Doc. 3698

The IBM 3581-L17 and IBM 3581-L13 are functionally identical, as are the IBM 3581-H17 and IBM 3581-H13. The only difference is that the IBM 3581-L13 and the IBM 3581-H13 have a three-year Customer Element Exchange warranty.

Note: Although the IBM TotalStorage Ultrium Tape Autoloader 3581 provides the capability for high tape performance, other components of the system may limit the actual performance achieved. Also, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

5.1.1 Feature codes

The IBM 3581 can be ordered and/or upgraded with the following feature codes (Table 5-1). We have not included the various cabling options; refer to the product publications for detailed information about configuring and ordering the IBM TotalStorage Ultrium Tape Autoloader 3581.

Table 5-1 IBM 3581 feature codes

Feature Code	Description	Comments
1748	Custom QuickShip	
7003	5U rack mount option	Plant or field install
7004	Barcode reader	
8001	One 100GB data cartridge	Plant only, see Media section for details.
8002	One cleaning cartridge	Plant only, see Media section for details.
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9400	Attached to AS/400	
9600	Attached to AIX	

5.1.2 Access mode

The IBM 3581 can be operated in sequential or random-access modes. In sequential mode, the IBM 3581 loads cartridges one after another, controlled by

10654
LA

the hardware when it receives the unload command from the host server. In random-access mode, the IBM 3581 relies on application software for cartridge management.

5.1.3 SCSI devices

Although it has only a single tape drive, the 3581 appears as two SCSI devices on the SCSI bus. In other words, the autoloader and the drive have separate SCSI addresses.

The IBM 3581 only operates on a single path, and control of the autoloader is handled by a single server. Connection to multiple servers can be achieved when using SAN technology and appropriate application software for cartridge management, such as IBM Tivoli Storage Manager V3.7 or higher.

5.1.4 Adding and removing cartridges

The IBM 3581 does not have a cartridge I/O station. In order to insert and remove cartridges from the slots you have to open the autoloader door. The IBM TotalStorage Ultrium Tape Autoloader 3581 can contain up to seven tape cartridges:

- Five cartridges in the front, slots 1 through 5
  (referred to as front slots; see label 1 in Figure 5-2)
- Two cartridges in the rear, slots 6 and 7
  (referred to as rear slots; see label 2 in Figure 5-2)

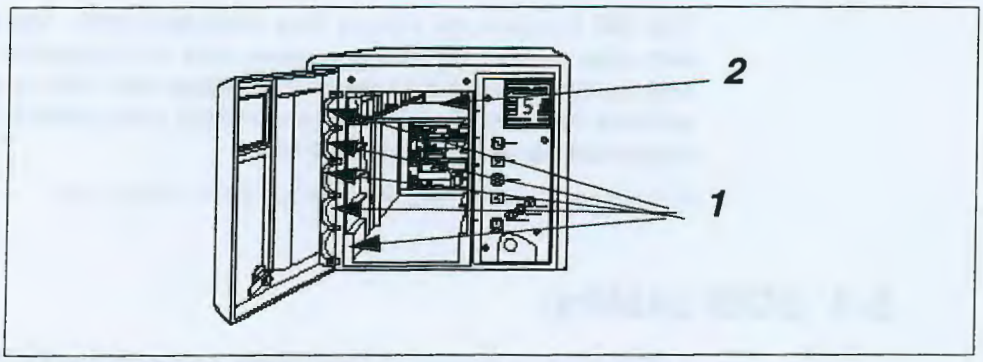


Figure 5-2 IBM 3581 cartridge slots

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1309
Doc 3698

5.1.5 Operation

The IBM 3581 autoloader is designed for easy, unattended operation. An optional barcode reader makes tape inventory tasks more efficient. Indicators on the operator's panel provide information about:

- Power
- Autoloader and drive activity
- Error status
- Message information

Push buttons provide display, mode, and power controls.

5.2 SCSI attachments

The SCSI interface (HVD or LVD) on each IBM TotalStorage Ultrium Tape Autoloader 3581 is chosen by selecting the appropriate model number (H17/13 or L17/13).

The IBM TotalStorage Ultrium Tape Autoloader 3581 can be attached to iSeries, AS/400, pSeries, RS/6000, xSeries, Netfinity, HP, Sun, UNIX, and PC servers that support Ultra/Wide SCSI HVD and Ultra2/Wide SCSI LVD interface specifications. The interface you choose will depend on the available adapter in the host, which must be of the same type as the drive interface.

SCSI cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code should also be specified.

The IBM TotalStorage Ultrium Tape Autoloader 3581 also may be compatible with other servers, operating systems, and SCSI adapters. Contact your local IBM representative for a current list of supported open system configuration and software vendors. You also may refer to the Interoperability Matrix (List of Supported Servers) on this Web site:

`http://www.storage.ibm.com/tape/lto/3581/3581opn.pdf`

5.3 SCSI cabling

A SCSI cable is required for each 3581 connection to a SCSI bus. A single 2.5 m SCSI cable is available as a no-charge feature; if an alternate length is required it should be included in the initial order. A SCSI terminator is included with each autoloader. An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) also may be required for attachment to particular server adapters.

10652
A.

5.3.1 Cables

A single SCSI cable is available as no-charge feature #9702 or #9703 only with the initial IBM 3581 order. These no-charge features cannot be ordered later as a miscellaneous equipment specification (MES); however, the same cables can be ordered later as chargeable MES upgrades using feature codes #5302 and #5602. Feature #9702 supplies a 2.5 m SCSI cable with HD68 connectors at each end; feature #9703 differs in that one end has a VHDCI connector.

Additional SCSI cables are available as optional features on the IBM 3581 for LVD and HVD attachment to host adapters:

- Feature #5301, 0.4 m (1.4 feet) SCSI cable
- Feature #5302, 2.5 m (8.2 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The cables can be used with an HVD Ultra SCSI bus or LVD Ultra2 SCSI bus and have an HD68 connector on each end. A SCSI terminator is included with each Ultrium autoloader.

The following cables differ in that they have a VHDCI connector at one end:

- Feature #5602, 2.5 m (8.2 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 2 5m (82 feet) SCSI cable

5.3.2 Interposers

An interposer is required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries adapter #6501.
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable.

  This interposer (a 0.3 m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1310
3698
Doc

5.3.3 SCSI length limitations

The IBM 3581 has one SCSI ID for the drive and one for the loader, so the SCSI interconnection is multi-drop. This means that the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

5.4 Upgrades and optional features

The IBM 3581 H17/13 and L17/13 are single tape drive autoloaders and cannot be upgraded to any other models.

Two additional optional features are available:

- Feature #7003, 5U Rack Mount Option
  The IBM 3581 can be installed as a stand-alone single unit, or two units can be mounted side-by-side in a standard 19-inch rack, requiring 5 EIA units of rack space. This chargeable feature provides the necessary hardware to mount the autoloader in the rack.
- Feature #7004, Barcode Reader
  This optional chargeable feature enables the IBM 3581 autoloader to read cartridge information contained in a barcode label on the IBM Ultrium cartridges. User-installed application software provides the inventory management functions enabled by the barcode reader feature.

Note: Installing feature #7004 reduces the autoloader capacity to six data cartridges. The barcode reader connects to the interface connector on the inside top panel of the IBM 3581. This location prevents you from using cartridge storage slot 1 (see Figure 5-2 on page 97). When you install the barcode reader, you reduce the capacity of the autoloader to six cartridge storage slots. The front storage slots are still numbered 1 through 5, but the autoloader's menu functions and the server's application software cannot select or use slot 1.

This is illustrated by observing that, with the barcode reader installed, the operator LOAD SLOT function uses storage slots 2 and 3 as the cartridge source locations to load slots 6 and 7; without the barcode reader installed, the LOAD SLOT function uses storage slots 1 and 2 as the source locations. See Figure 5-2 on page 97 for slot locations.

10650
CA

5.5 Environmental specifications

The IBM 3581 is a medium-sized desktop or stand-alone unit that optionally can be integrated into a standard 19" rack for space optimization. Two IBM 3581s can be installed side-by-side in a rack using 5 EIA space units.

5.5.1 Physical dimensions

The IBM 3581 models H17/13 and L17/13 are medium-sized single tape drive autoloaders:

- Width: 21.9 cm (8.62 in)
- Depth: 58.1 cm (22.87 in)
- Height: 19.0 cm (7.48 in)
- Maximum weight: 13.0 kg (28.7 lbs)

5.5.2 Operating environment

The IBM 3581 can be installed in a normal office environment and does not need to be in a specialized machine room.

5.6 Host platforms and device drivers

The following no-charge specify codes indicate the server platform to which the IBM 3581 is attached.

- #9210, attached to HP-UX
- #9211, attached to Sun system
- #9212, attached to Windows NT system
- #9213, attached to other non-IBM system
- #9400, attached to iSeries system
- #9600, attached to RS/6000 system

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3581). Sometimes the driver code is supplied as part of the operating system code (such as, in OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1311
3698
Doc.

Ultrium 1

The IBM TotalStorage Ultrium Tape Autoloader is shipped with device drivers to support Ultrium 1 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.2 or later
- Sun Solaris 2.6, 7, and 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- Windows 2003
- HP-UX 11.0
- OS/400 V4R4

Tip: The device driver CD or diskette that is shipped with the IBM 3581 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Therefore you should always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

5.6.1 Device driver installation

Install the IBM device drivers for the IBM 3581 as follows:

- If you intend to use the IBM 3581 with a storage management application (such as Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3581.
- If you do not intend to use the IBM 3581 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the autoloader. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide*, GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3581 with a commercial software application, IBM recommends that you install an IBM-supplied device driver *only* if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, conflicts could occur over which driver controls the tape subsystem. Many examples of using the Ultrium drives are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

10648
A.

5.7 Storage applications

The software to manage the IBM 3581 is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software vendors. A list of compatible software is available at:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1 and Ultrium 2 support and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more-detailed information of specific versions and platforms supported.

5.8 Performance considerations

For best performance, it is recommended to attach only one tape drive per SCSI bus. This may not be a realistic objective, but minimizing the number of devices per bus will improve performance. Attaching other SCSI devices on the same SCSI bus as the IBM 3581 drive may affect performance of those devices.

iSeries configurators allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape drive on an input/output port may affect system performance.

Although the compression technology can increase the amount of data stored on the media, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

5.9 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each autoloader order[3]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3581:

- Feature #8001 provides a single 100 MB Ultrium Data Cartridge.
  It is a chargeable feature, and a maximum of seven can be ordered.
- Feature #8002, provides a single Ultrium Cleaning Cartridge.
  It is a chargeable feature, and a maximum of three can be ordered.

[3] All media and cleaning cartridges are warranted separately from the IBM TotalStorage Ultrium Tape Autoloader 3581.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1312
3698
Doc.

Subsequent to the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about ordering supplies and cartridges, with or without labels.

5.10 IBM 3581 initial setup

The following section covers some of the major items required to implement, manage, and operate the IBM 3581 tape library. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the Setup and Operator Guide and to the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

5.10.1 SCSI ID

The IBM 3581 consists of two SCSI devices: the autoloader and the drive. The default settings for the SCSI IDs as displayed on the message display panel are LdR Id 1[4] (for the autoloader) and dRV Id 3 (for the drive). Depending on your requirements, you may need to change the SCSI ID default settings for your installation. When setting a SCSI ID:

- Do not select an ID that is already in use.
- Do not select the SCSI ID of the server SCSI adapter card. The SCSI ID of the server SCSI adapter card is usually higher than any device on the SCSI bus. Generally, the SCSI ID for the server adapter is set to 7.
- Do not use F, as it is reserved for internal use by the SCSI library.
- Unless you choose another operation, the IBM 3581 times out 30 seconds after each operation and LdR REAdY appears in the message display (label 1 in Figure 5-3 on page 106).
- Functions and messages in the message display can only be scrolled forward. To select a previously viewed function, continue to scroll through the choices until the function that you want appears on the message display.
- As with the IBM 3580, the IBM 3581 can be part of a SCSI chain. The same rules apply for SCSI addresses as for the IBM 3580.

Refer to the Setup and Operator Guide for details about determining and changing the SCSI IDs.

[4] The message display panel displays a D as a lower case letter so we have shown the message as it would appear.

10646
A-

5.10.2 Element numbers

Element numbers (also called element addresses) identify the physical location within the autoloader. This information is required by storage management applications such as the Tivoli Storage Manager.

The three types of elements in the IBM 3581 are shown in Table 5-2:

Table 5-2 IBM 3581 element numbers

Element	Element number
Picker (media transport element)	57 hexadecimal
Tape drive (data transfer element)	52 hexadecimal
Storage element	01 - 07 hexadecimal

The IBM 3581 has one storage element for each of the cartridge storage slots.

A host application controls movement within the autoloader by issuing one of these SCSI commands:

- MOVE MEDIUM

  This SCSI command tells the autoloader to move a cartridge from the source element to the destination element. The elements are identified using the element numbers shown in Table 5-2. So, for example, a MOVE MEDIUM command could be issued to tell the library to move a cartridge from the picker to the drive.

- POSITION TO ELEMENT

  This SCSI command positions the picker to a specified element number.

5.10.3 Operator displays and buttons

Management of the IBM 3581 is performed by using the status lights, message display panel, and push buttons on the control panel behind the front door.

Status lights

The IBM TotalStorage Ultrium Tape Autoloader 3581 features three status lights on the operator panel (label 2 in Figure 5-3 on page 106):

- POWER: The green POWER light comes on whenever you turn on the power.
- ACTIVITY: The amber ACTIVITY light indicates robotic or drive activity. A slowly blinking light indicates robotic activity; a rapidly blinking light indicates drive activity.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1313
Doc 3698

- ALARM: The red ALARM light comes on whenever an error occurs. To resolve the error refer to the Setup and Operator Guide.

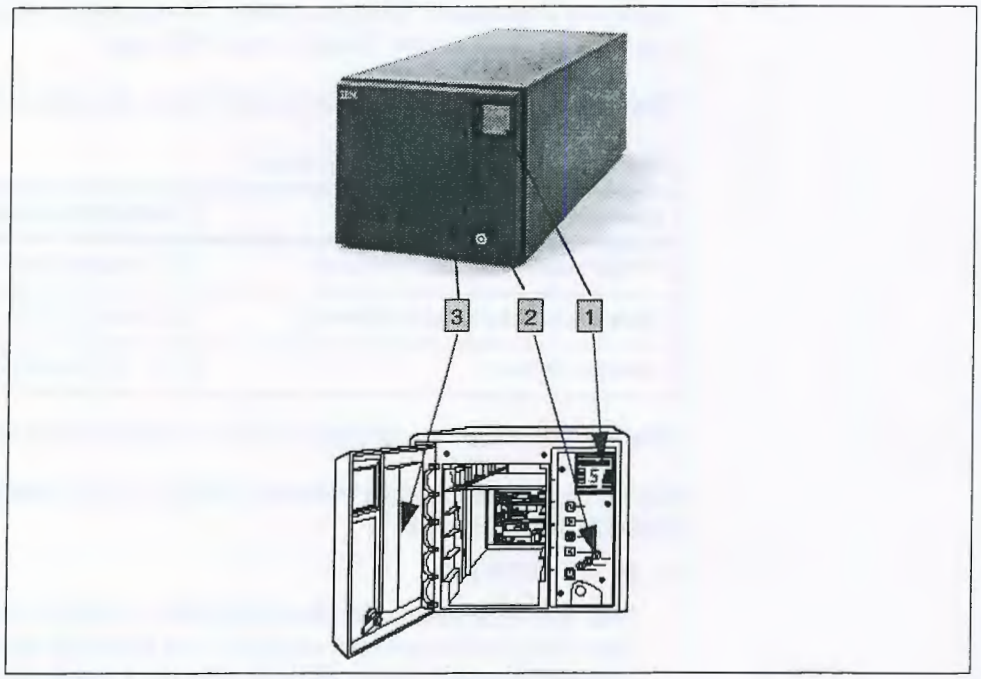


Figure 5-3 IBM 3581 front view

5.10.4 Message display

The IBM TotalStorage Ultrium Tape Autoloader 3581 offers a one-line, 10-character front panel with a liquid crystal display (LCD) that provides operational information as well as diagnostics and messages.

The LCD message display (label 1 in Figure 5-3) provides information about the status of the IBM TotalStorage Ultrium Tape Autoloader 3581 and any error conditions. When in an idle (non-operating) state, the autoloader message panel displays LdR REAdY. In addition, the following characters (shown in Figure 5-4 on page 107) may appear on the left side of the display:

- DC: Indicates that data compression is selected on the drive.
- WP: Indicates that a write-protected data cartridge is loaded in the drive.
- CT: Indicates that the drive head needs to be cleaned.

The large field in the center of the display indicates the number of the storage slot from which the picker removed a cartridge for loading into the drive.

106644
A.

Whenever an error occurs, E displays in this field and the error message is displayed on line 1.

The activity bars on the right (in conjunction with the activity light) indicate robotic and drive activity:

- The bottom bar blinks when no activity is taking place.
- A slow interval between the bars appearing and disappearing indicates robotic activity.
- A fast interval between the bars appearing and disappearing indicates drive activity.

The seven numeric fields at the bottom of the display indicate the current cartridge inventory. Each will appear only if a cartridge is present in that storage slot, as shown in Figure 5-4.

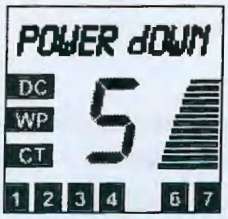


Figure 5-4 IBM 3581 message display

5.10.5 Drive status messages

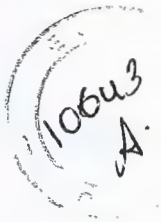
During operation, the IBM 3581 places messages about the drive's status in the message display. These messages can appear:

- CLEANING: The drive is cleaning the head with the cleaning cartridge.
- EJECTING: The drive is unloading the tape.
- ERASING: The drive is erasing the tape.
- LOADING: The drive is loading the tape.
- LOCATING: The drive is locating the position on the tape.
- READING: The drive is reading from the tape.
- REWINDING: The drive is rewinding the tape.
- WRITING: The drive is writing to the tape.

If an error occurs during operation, the IBM 3581 halts the current operation and displays an error code in the message display. The following list provides the most common errors codes and gives a description of each:

- CT FAILED: Cleaning tape failed to clean drive.
- DEST FULL: The destination location was full.
- DRIVE BUSY: The drive is busy and cannot unload the tape.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1314
3698
Doc



- DRIVE FULL: The drive was full.
- DRIVE PGRM: The attempt to set drive parameters failed.
- DRIVE POST: The drive failed its Power-On Self Test (POST).
- FRONT SLOT: A front slot sensor was not tripped.
- FRONT TAPE: A front tape sensor was not tripped.
- LDR INIT: The autoloader could not complete its initialization.
- PCKR EMPTY: The picker was empty.
- PCKR FULL: The picker was full.
- REAR SLOT: A rear slot sensor was not tripped.
- REAR TAPE: A rear tape sensor was not tripped.
- ROBOT POST: The robotics failed its Power-On Self Test (POST).
- SRC EMPTY: The source location was empty.
- SLOT EMPTY: No slot beam was detected.
- PWR SWITCH: The front power switch was pressed.
- SLOT FULL: A cartridge was already in the slot.

This list is not complete. See the Setup and Operator Guide for the full error list.

5.10.6 Control buttons

The control buttons are push buttons on the operator panel that let you interact with the menus on the message display (Figure 5-5 on page 109):

MODE:	Scrolls through the commands that you can use to operate the IBM 3581 (label 1 in Figure 5-5 on page 109).
NEXT:	Highlights the next item or value in the currently displayed menu (label 2 in Figure 5-5 on page 109)
SELECT:	Selects the currently displayed operation (label 3 in Figure 5-5 on page 109).
PREVIOUS:	Highlights the previous item or value in the currently displayed menu (label 4 in Figure 5-5 on page 109).

To operate a button, press and release it. You can use the control buttons to:

- Load a tape cartridge into a drive (LOAd dRV)
- Eject a tape cartridge from the drive and put it into the storage slot that it was loaded from (EJECT dRV)
- Load slot 6 from slot 1, or load slot 7 from slot 2 (LOAD SLOT)
- Move a cartridge from slot 6 to slot 1 or from slot 7 to slot 2 (EJECT SLOT)
- Eject a tape cartridge that was left in the media picker into an empty destination slot (EJECT PCKR)
- Set the SCSI ID of the autoloader or the drive (SET SCSI)

1064
A-

Note: The procedure for loading slots 1 through 5 differs from loading slots 6 and 7. If you are loading seven cartridges, load slots 6 and 7 first. See "Inserting a Cartridge into Slots 6 and 7" of the chapter "Operating the IBM 3581 Tape Autoloader" in the Setup and Operator Guide, which also contains a complete list of commands.

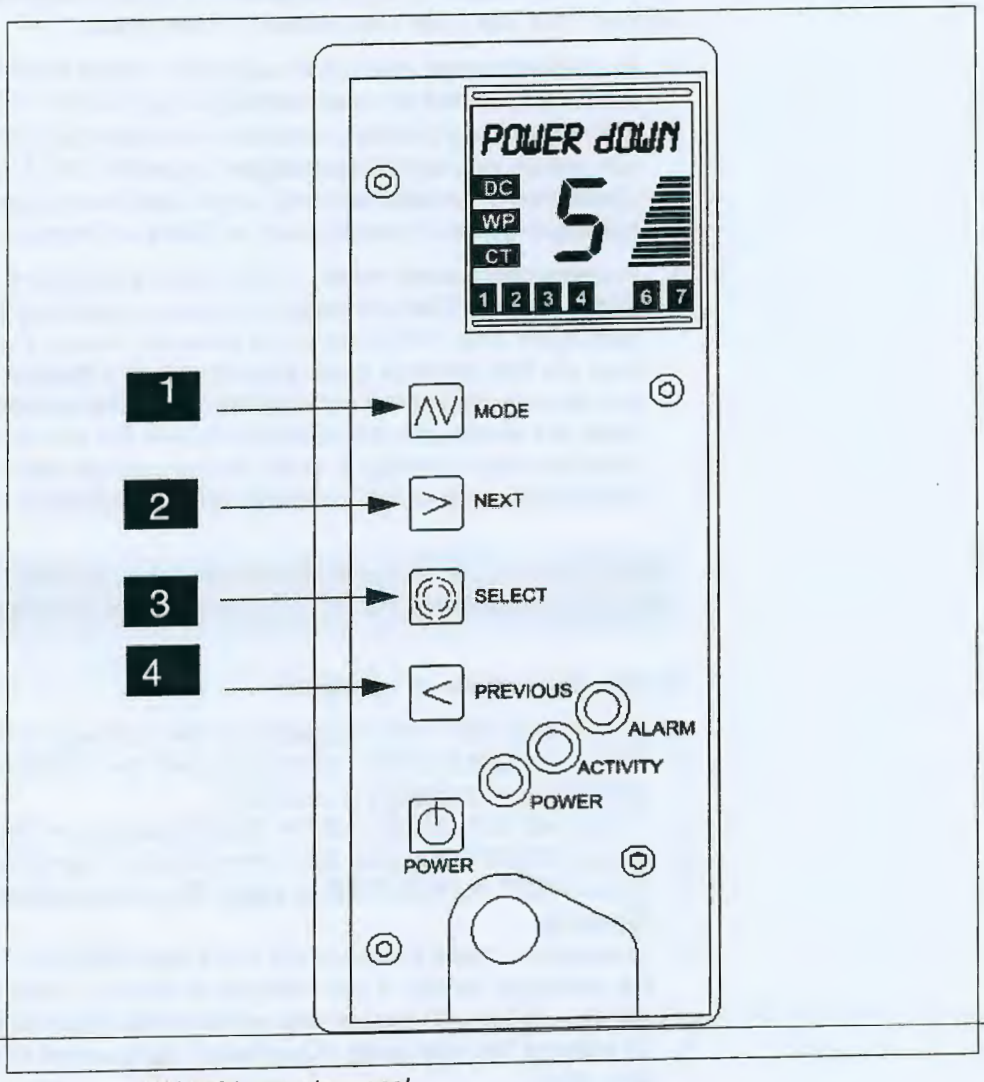


Figure 5-5 IBM 3581 operator panel

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1315
3698
Doc

5.10.7 Operating modes

The IBM 3581 operates in both random access mode (in which the server's application software manages the cartridges) and sequential access mode (in which the autoloader's firmware manages the cartridges).

Change between random and sequential mode through the *Diagnostic Menus.*

Select CHG MODE to toggle between the random access and sequential access modes. The IBM 3581 can operate in either mode:

- In random access mode, the autoloader allows the server's application software to select any data cartridge in any order. You can logically divide cartridge usage to satisfy particular data storage needs. For example, you can assign one or more cartridges to specific data functions (such as certain directories or network servers), or you can assign specific cartridges to individual users or groups (such as Sales or Engineering).
- In sequential access mode, all cartridges present are considered to be a single volume. The autoloader's firmware predefines the selection of the cartridges. After initialization, the firmware causes the autoloader to always load the first cartridge found (counting from 1 through 7) into the drive. After the server's application software has filled this cartridge and unloaded the drive, the autoloader automatically returns the cartridge to its storage slot and loads the next cartridge in order. Empty storage slots are ignored. The autoloader continues this process until the volume is full.

Note: While in sequential access mode, the autoloader's robotics are not logically connected to the SCSI bus and do not respond to SCSI commands.

To change the mode of operation:

1. Ensure that LdR REAdY appears on the message display.
2. Press and hold the NEXT button and then the MODE button until dIAG MENU displays (approximately 5 seconds).
3. Press and hold MODE until CH MOdE appears on the message display.
4. Press SELECT to display the current mode of operation.
5. Press NEXT or PREVIOUS to toggle the mode between SEQUENTIAL and RANdOM.
6. Choose the mode that you want and press SELECT. CYCLE PWR blinks on the message display. If you changed to random mode, LdR REAdY then displays; if you changed to sequential mode, SEQ REAdY then displays.
7. To activate the new mode of operation, cycle power (turn off, then on) to the IBM 3581.

The complete list of mode set-up commands is in the Operator and Setup Guide.

10640
CA.

5.11 Drive cleaning

All IBM Ultrium tape drives have an integrated cleaning mechanism that brushes the head at load time and again when unloading a cartridge. There is also a cleaning procedure using a special cleaning cartridge.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

The IBM 3581 internal tape drive determines when the head needs to be cleaned and alerts you by displaying CT on the message display (label 1 in Figure 5-3 on page 106). This is the *only* occasion when a cleaning cartridge should be used. The IBM 3581 supports three methods of cleaning the drive:

- Host cleaning
  Host cleaning enables the server software to detect the need to clean an Ultrium Tape Drive and to control the cleaning process. The cleaning cartridge must be stored in one of the available storage slots within the 3581.
- Automatic cleaning (AUTOCLEAN)
  Automatic cleaning enables the 3581 to automatically respond to any tape drive's request for cleaning and to begin the cleaning process. Automatic cleaning makes the cleaning process transparent to any host application using the autoloader. If the server application does not support the host cleaning function, use the autoclean function.
- Manual cleaning
  Manual cleaning requires you to select a menu option from the autoloader's display. Manual cleaning is always supported, regardless of whether host cleaning or automatic cleaning is enabled or disabled.

In all methods, the autoloader performs the cleaning after you unload the data cartridge from the drive and before the next load.

Note: Whenever you enable host application cleaning or the autoloader's autoclean function, the tape capacity of the autoloader is reduced to six tapes without the barcode reader and to five cartridges with the barcode reader feature installed. The extra slot is used for storing the cleaning cartridge within the IBM 3581.

Proper instructions for cleaning the IBM 3581 tape drive can be found in "Performing Diagnostic and Maintenance Functions" in the Setup and Operator Guide.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1316
Doc: 3698

5.12 Firmware upgrade

Each IBM Ultrium Tape drive and library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the latest firmware is installed on your IBM LTO Autoloader. As the IBM 3581 is designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed.

Determine the latest level of firmware available from the Web site:

```
http://www-1.ibm.com/support/docview.wss?rs=541&context=STCVQ5N&q=ssg1*&uid=ssg
1S4000042&loc=en_US&cs=utf-8&lang=en+en
```

Follow the instructions for updating your firmware in the *IBM 3581 Ultrium Tape Autoloader Setup, Operator, and Service Guide*, GA32-0412, or from:

```
http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_dri
vefw
```

10638
A

6

IBM TotalStorage Ultrium Tape Library 3582

The newest member of the IBM Ultrium family is the IBM TotalStorage Ultrium Tape Library 3582, shown in Figure 6-1 on page 114. It is a high-performance, reliable, scalable tape subsystem. Designed for tape automation, the IBM TotalStorage Ultrium Tape Library 3582 (IBM 3582) can be attached to iSeries, pSeries, xseries, Intel (running Windows or Linux), Sun SPARC, Hewlett-Packard, and other open systems using SCSI or Fibre Channel attachment. It uses IBM Ultrium 2 tape drives for faster data transfer and reliability in automated library service. Each aspect of the library subsystem has been optimized for repeated, reliable unattended tape handling.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1317
Doc. 3698

6.1 Model description

The IBM 3582 tape library houses one or two IBM Ultrium 2 tape drives, which each have a native data transfer rate of 35 MBps and a cartridge capacity of 200 GB. The drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm that provides an effective data rate of up to 70 MBps and a cartridge capacity of up to 400 GB (with 2:1 compression) on IBM Ultrium 2 media. Multiple drive models provide additional enhanced functions such as faster transfer of data, simultaneous backup, concurrent read-write operations, and fault tolerance through Control Path Failover.

The IBM 3582 has one I/O slot plus additional cartridge capacity of 23 slots (24 slots in all), allowing a native capacity of 4.8 TB of uncompressed data. With compression (assuming 2:1), the IBM 3582 can store 9.6 TB of data. These capacities assume that the I/O slot has been configured as an additional storage slot, increasing the overall library capacity.

The IBM 3582 is an excellent high-performance, entry-level choice for entry-level and midrange systems.

Figure 6-1 IBM TotalStorage Ultrium Tape Library 3582

The IBM TotalStorage Ultrium Tape Library 3582 supports three Ultrium 2 drive types: Ultrium 2 LVD, Ultrium 2 HVD, and Ultrium 2 FC. The drives can be intermixed. The IBM 3582 comes standard with multi-path architecture and the ability to partition the library into two logical libraries. The library can be configured as a stand-alone unit or mounted in an industry-standard 19-inch

10636
A-

rack. Additional optional features include Control Path Failover for AIX and a Remote Management Unit/Specialist for remote library management.

Table 6-1 IBM 3582 model summary

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	IBM Ultrium tape drives
3582-L23	23[a]	4.4 TB	8.8 TB	1-2

a. Plus one I/O Station slot that can be assigned as a storage slot. If this is done, the library capacity is 4.8 TB (9.6 TB compressed).

6.1.1 Tape drives

The IBM 3582 libraries use IBM LTO Ultrium 2 tape drives. It is mandatory to have at least one IBM Ultrium drive installed in the library. An additional drive may be added at the initial order or as a field upgrade performed by the customer.

The installed drives may be any mixture of LVD, HVD, or FC. The drives are ordered for plant or field installation using chargeable feature codes:

- Feature #8103 provides one IBM Ultrium 2 tape drive with a Low Voltage Differential (LVD) Ultra2/Wide SCSI Connection.
- Feature #8104 provides one IBM Ultrium 2 tape drive with a High Voltage Differential (HVD) Ultra/Wide SCSI Connection.
- Feature #8105 provides one IBM Ultrium 2 tape drive with a Native 2 Gb Fibre Channel Connection.

Each IBM Ultrium tape drive contains the electronics and logic for reading and writing data, control of the tape drive, management of the data buffer, and error-recovery procedures. All tape drives are packaged as a common assembly that is a Field Replaceable Unit (FRU), designed for quick removal and replacement.

6.1.2 Cartridge storage

As well as the installed tape drives, the library enclosure contains cartridge storage slots, arranged in two rows. The row toward the front of the library is made of two removable magazines of seven slots each. The row toward the rear of the library contains nine slots (Figure 6-3 on page 116). The magazines are designed so that tape cartridges can only be inserted in the proper orientation. Once inserted, the tape cartridges will be retained in the magazine so that they remain in place even when the magazine is inverted and shaken lightly. The magazines can only be inserted one way into the mounting columns in the library.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1318
Doc. 3698

In Figure 6-2, one magazine is loaded and the other is removed.

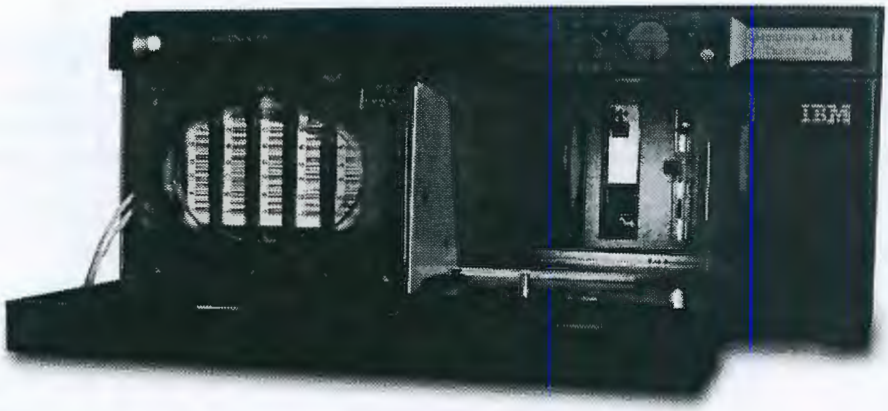


Figure 6-2 IBM 3582 seven-slot magazines

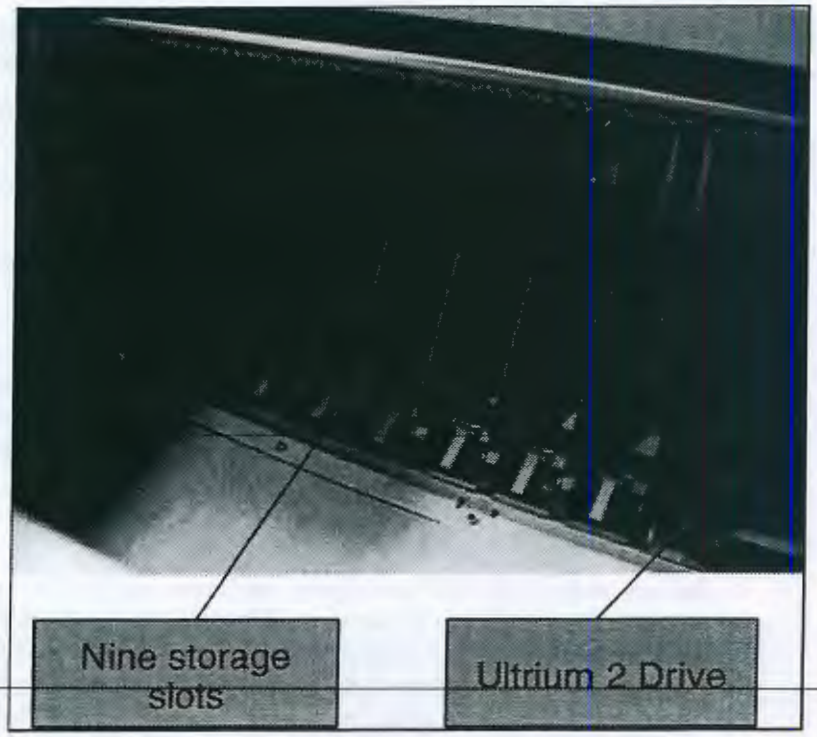


Figure 6-3 IBM 3582 rear-mounted storage slots

10634
A.

6.1.3 Barcode scanner

A barcode scanner is provided as standard with the IBM 3582-L23, and it does not affect the slot capacity of the libraries. The barcode scanner is used during the inventory process to locate all cartridges inserted into the library. This action is repeated every time the front door is opened to ensure that the inventory is updated if a cartridge has been manually added, moved, or removed while the door was open.

6.1.4 I/O station

This facility enables the insertion and ejection of cartridges without interrupting the normal operation of the library. There is a single-slot I/O station where a cartridge can be inserted or ejected by opening the I/O station door.

6.1.5 Robotic system

In conjunction with the library control microcode, the robotic system identifies and moves cartridges between the storage slots, tape drives, and the I/O station. It has a number of components:

- A cartridge picker for placing cartridges in storage slots, tape drives, or the I/O station
- A bar code scanner used to set up the library initially when it identifies the types of storage arrays and tape drives installed in the library, and in normal operation for reading the external labels on the cartridges, when it locates and categorizes all cartridges installed in the library
- X-axis and Z-axis drive motors for moving the picker assembly inside the library enclosure

6.1.6 Library control and operation

The library control unit contains the electronics and logic for autochanger operations. It controls all operations in the IBM 3582 library, including the interaction between the library and operators. The control unit Licensed Internal Code creates and maintains the library configuration, the physical location of the robotic system, and the inventory of cartridges. The database is kept in the flash memory of the library control hardware.

Requests issued from the server result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges to and from the tape drives and for inserting and ejecting cartridges. The host has records of the physical location of a cartridge in the library, and the physical location is also managed by the library.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1319
3698
Doc.

In addition to requesting movement of cartridges in the library, the host can obtain status, performance, configuration information, and information about the cartridges stored in the IBM 3582 tape library.

Each cartridge must have a machine- and operator-readable external barcode label to identify a media cartridge in the library during initial inventory and any time a cartridge is added to the library. The library stores the physical location of the cartridge in an inventory database based on the cartridge label. All host application requests for operations involving movement or use of a cartridge need only reference the physical location of the cartridge (using an element number as described in 6.10.2, "Identifying library location element numbers" on page 125) for the library to perform the request.

6.1.7 Operator panel

An LCD operator control panel on the front of the machine provides status information and menu options. From this panel the operator can initiate actions such as moving and loading tape cartridges or invoking diagnostics.

6.1.8 Maintenance

The cartridge storage slots, cartridge picker, and tape drives are accessed for maintenance purposes by opening the front door of the library. The tape drives, power supplies, and host interface board are reached from the back of the library.

6.2 Feature codes

The IBM 3582 can be ordered and/or upgraded with the feature codes shown in Table 6-2. We have not included the various cabling options; refer to the product publications for detailed information about configuring and ordering.

Table 6-2 IBM 3582 feature codes

Feature	Description	Comment
1660	RMU/Specialist	
1680	Control Path Failover	
2200	Standalone Kit	
7003	Rack Mount Kit	
8101	1 data cartridge	Plant only, see Media section for details.

10632
A

Feature	Description	Comment
8002	1 cleaning cartridge	Plant only, see section Media for details.
8103	Ultrium 2 LVD drive	
8104	Ultrium 2 HVD drive	
8105	Ultrium 2 Native FC drive	
8203	CSU Ultrium 2 LVD drive	Customer Setup
8204	CSU Ultrium 2 HVD drive	Customer Setup
8205	CSU Ultrium 2 Native FC drive	Customer Setup
8110	20 data cartridges	
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9215	Attached to Linux	
9400	Attached to AS/400	
9600	Attached to AIX	

6.3 Physical attachments

The IBM 3582 tape library can be attached to IBM iSeries, IBM pSeries, IBM RS/6000 and SP systems, IBM xSeries and non-IBM servers, workstations, and personal computers that support the Ultra/Wide SCSI HVD, Ultra2/Wide SCSI LVD, and Fibre Channel interface.

SCSI cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code also should be specified.

The IBM 3582 may be compatible with other servers, operating systems, and SCSI adapters. Contact your local IBM representative for a current list of supported open system configuration and software vendors, or go to:

`http://www.storage.ibm.com/tape/lto/3582/3582opn.pdf`

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 1320
Doc. 3698

6.4 SCSI cabling

A SCSI cable is required for each library connection to a SCSI bus. If no cable is available, one should be specified on the initial order for each library or drive. A SCSI terminator is included with each cable. An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) also may be required for attachment to particular server adapters.

6.4.1 Cables

A host-to-library SCSI cable is available as no-charge feature #9704 or #9705 specified only with the initial IBM 3582 order. One of these cables is supplied with each library ordered. Features #9704 and #9705 cannot be ordered as a miscellaneous equipment specification (MES) for later installation; however, the same cables may be ordered as chargeable MES upgrades after installation by using feature codes #5305 and #5604. Feature #9704 supplies a 4.5 m SCSI cable with an HD68 connector at one end and a VHDCI connector at the other end; feature #9705 supplies a 5 m SCSI cable with HD68 connectors at each end.

Additional SCSI cables are available as optional features on the IBM 3583 for LVD and HVD attachment to host adapters:

- Feature #5302, 2.5 m (8.2 feet) SCSI cable
- Feature #5303, 0.7 m (2.3 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The cables can be used with an HVD Ultra SCSI bus or LVD Ultra2 SCSI bus and have an HD68 connector on each end. A SCSI terminator is included with each Ultrium library.

The following cables differ in that they have a VHDCI connector at one end:

- Feature #5602, 2.5 m (8.2 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 25 m (82 feet) SCSI cable

10630
CA

6.4.2 Interposers

An interposer is required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries to adapter #6501
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable.

  This interposer (a 0.3m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

6.4.3 SCSI length limitations

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection. If using multi-drop interconnection, then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using point-to-point or multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

6.5 Environmental specifications

The IBM TotalStorage Ultrium Tape Library 3582 is a stand-alone, medium-sized library unit that can be placed on a desk or in a rack.

The IBM 3582 has one or two drives and 23 cartridge slots, plus a single-slot I/O station. The physical dimensions are:

- Width: 45.5 cm (17.9 in)
- Depth: 65.4 cm (25.8 in)
- Height: 19.3 cm (7.7 in) for a stand-alone library on casters
- Maximum weight: 30.3 kg (66.7 lb) with two drives
- Four EIA units high (if rack-mounted)

6.6 Host platforms and device drivers

The following no-charge codes indicate the server platform to which the IBM 3582 is attached:

- Feature #9210 attached to HP-UX

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1321
3698
Doc.

- Feature #9211, attached to Sun system
- Feature #9212, attached to Windows NT or Windows 2000 system
- Feature #9213, attached to other non-IBM system
- Feature #9215, attached to Linux system
- Feature #9400, attached to iSeries system
- Feature #9600, attached to xSeries

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3582). Sometimes the driver code is supplied as part of the operating system code (such as in OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

The library is shipped with the device drivers to support the following operating environments at the minimal levels shown:

- AIX Versions 4.3.3 or later
- Sun Solaris 2.6, Solaris 7, or 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 (9215)
- Windows 2003
- HP-UX 11.0, 11.i (64 bit)
- OS/400 V5R1 or later
- Linux Red Hat 7.2 (32 and 64 bit kernels), Red Hat 7.3, Red Hat Advanced Server 2.1, SuSE Linux Enterprise Server Update

Tip: The device driver CD or diskette that is shipped with the IBM 3582 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

6.6.1 Device driver installation

Install the IBM device drivers for the IBM 3582 as follows:

- If you intend to use the IBM 3582 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3582.
- If you do not intend to use the IBM 3582 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI*

10628
A.

Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3582 with a commercial software application, IBM recommends that you install any IBM-supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples of using the Ultrium drives are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

6.7 Storage applications

The software for managing the IBM 3582 is not provided with the library. It is not really feasible to use the IBM 3582 without some additional application software to manage the slots and cartridge inventory. Additional software support is available through library management software products, which can be obtained separately from IBM, IBM Business Partners, or independent software providers. A list of compatible software is available at the Web site:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1/2 support and specific Ultrium models and attachment methods. Contact your storage application vendor for more-detailed information about specific versions and platforms supported.

6.8 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each 3582 drive order[1]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3582:

- Feature #8101 provides a single 200 GB Ultrium 2 Data Cartridge. Up to 19 #8101 features can be ordered. The cartridges come with a barcode label but it is not affixed.
- Feature #8002 provides a single Ultrium Cleaning Cartridge. It is a chargeable feature, and a maximum of three can be ordered.
- Feature #8110 provides a pack of twenty 200 GB Ultrium Data Cartridges with un-attached barcode labels.

[1] All media and cleaning cartridges are warranted separately from the IBM 3582.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1322
3698
Doc:

Subsequent to the initial order, additional supplies may be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about ordering supplies and cartridges, with or without labels.

6.9 Installation and performance considerations

iSeries configurations allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape library on an input/output port may affect drive performance.

Installing more than one Ultrium drive on a SCSI bus may affect tape drive performance. For optimal performance, it is recommended that no more than one IBM Ultrium drive be attached to an individual SCSI bus.

Intermixing of other SCSI devices on the same SCSI bus as the IBM 3582 Ultrium tape library may affect performance of those devices.

While IBM Ultrium tape drives provide the capability for high tape performance, other components of the system may limit the actual performance achieved. The compression technology used in the tape drive can typically double the amount of data that can be stored on the media; however, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

The IBM 3582 Ultrium tape library has multi-path architecture; see 2.6, "Multi-path architecture" on page 46 for more information. This means the library can be logically divided into two separate physical libraries with a drive each, a seven-slot magazine each, and a pre-determined number of slots in the rear storage area of the IBM 3582. If the I/O slot is defined it can be shared.

6.10 IBM 3582 initial set-up

The following section covers some of the major items required to implement, manage, and operate the IBM 3582 tape library. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the *IBM 3582 Ultrium Tape Library Setup, Operator, and Service Guide*, GA32-0548.

10626
A

6.10.1 SCSI ID

The IBM 3582 has one or two SCSI devices/addresses: the two drives. The default settings for the SCSI IDs are 0 and 1. Depending on your requirements, you may have to change the SCSI ID default settings for your installation.

The IBM 3582 uses a path through one or more of the tape devices to access the tape library robot. The tape device is LUN 0, and the library robot will be LUN 1. A SCSI ID does not have to be set for the library robot.

The IBM 3582 is a SCSI target device and it can be connected to a single-ended, Low Voltage Differential or High Voltage Differential SCSI bus. The SCSI bus must be terminated, and a terminator is shipped with each library.

6.10.2 Identifying library location element numbers

To manipulate the media within the library, the host must reference each movement with source and target designations. This is done via element addressing, which specifies precisely which slots within the library are to be used. Table 6-3 shows the element addressing scheme used for the IBM 3582 tape library.

Table 6-3 IBM 3582 element numbering

Column	Element numbers
Picker	1
I/O station	16
Drives	256 - 257
Storage	4096 - 4116

Drives are addressed from bottom to top.

The I/O station is addressed from top to bottom. Storage slots are addressed from top to bottom, column by column.

6.11 Operator displays and buttons

Normally, the host issues commands to the IBM 3582 tape library. Operator control is provided via the Operator Panel. The operator is responsible for:

- Starting the IBM 3582 tape library
- Shutting down the IBM 3582 tape library
- Handling media

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1323
3698
Doc.

Refer to the IBM TotalStorage Ultrium Tape Library 3582 *Setup, Operator and Service Guide*, GA32-0458, for general procedures.

6.11.1 Operator Panel

The Operator Panel provides communication between the operator and the IBM 3582 tape library. Visual indications and push buttons enable the operator to control the IBM 3582 tape library.

As shown in Figure 6-4, the IBM 3582 tape library operator panel is divided into two areas:

1. Operator Panel Keyboard:
   The Operator Panel Keyboard is a five-button keypad that lets you control the library operations interactively. Using the Operator Panel, you can set library options, check library status, and diagnose errors.
2. Operator Panel Display:
   The Operator Panel Display is an LCD on the library front panel that is used to display icons and text.

Figure 6-4 IBM 3582 operator panel

Menu options

Figure 6-5 on page 127 shows the layout of the menu options on the operator panel.

10624
A

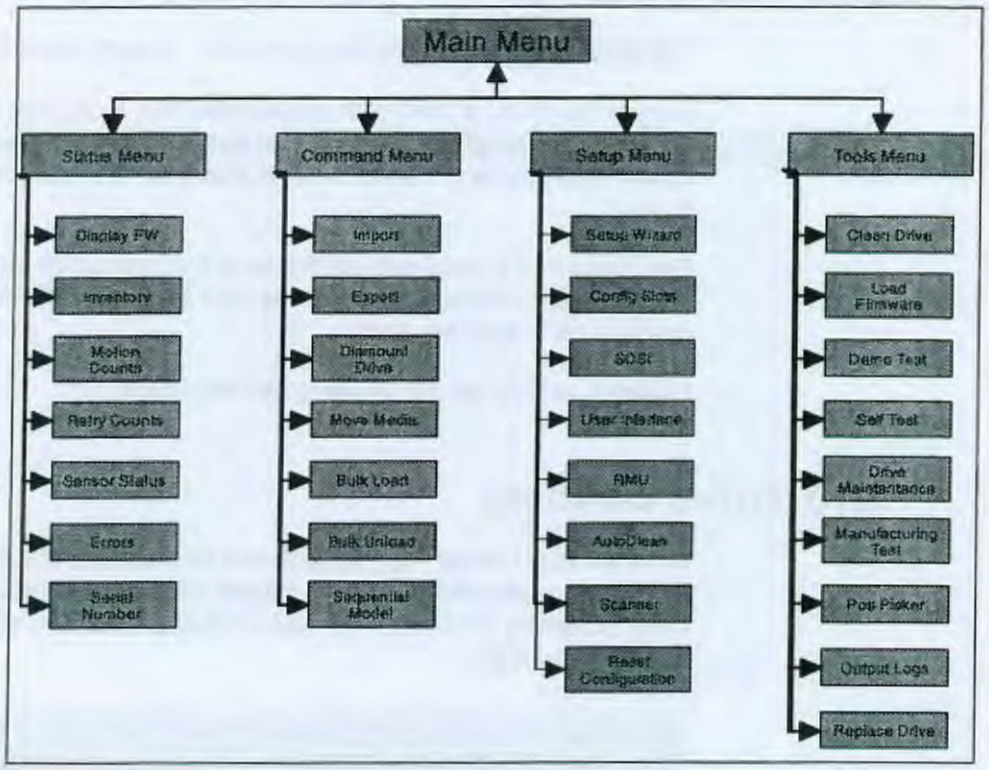


Figure 6-5 IBM 3582 top-level menu options

Each menu is accessible through the Operator Panel push buttons. Refer to the Operation chapter in the IBM TotalStorage Ultrium Tape Library 3582 *Setup, Operator and Service Guide*, GA32-0458, for all menu items.

Using commands that require an offline state

Some commands require that the library be in an offline state. If any such commands are attempted while the library is in an online state, the operator will be requested to take the library offline.

Operator intervention message

If a problem causes an operator intervention message to appear, refer to the Troubleshooting and Diagnostics section in the IBM TotalStorage Ultrium Tape Library 3582 *Setup, Operator and Service Guide*, GA32-0458.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1324
3698
Doc.

6.12 Library mode

The library operates in one of two modes: random mode or sequential mode.

Sequential mode is used with applications that recognize the tape drives but not the medium changer. Tape cartridge locations and loading are managed by the library, and data is written to tapes in the order in which they are stored in the library.

Random mode is used with applications that recognize the medium changer and drives. The application manages the tape loading, slot positioning, and the order in which cartridges are used.

Libraries usually are set up using random mode.

6.13 Drive cleaning

All of the IBM Ultrium Tape Drives have an integrated cleaning mechanism that brushes the head at load time and again when unloading a cartridge. Drives also have a cleaning procedure that uses a special cleaning cartridge, should this become necessary.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

A specially labeled IBM LTO Ultrium Cleaning Cartridge is supplied with each IBM 3582 tape library. The drive determines when the drive head needs to be cleaned, and alerts you by displaying CT on the message display.

6.14 Firmware upgrades

Each IBM Ultrium tape drive and tape library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the current firmware is installed on your IBM LTO tape drives and library. As the IBM 3582 is designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed. Determine the latest level of firmware available from the IBM Technical Support Web site:

```
http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/3582
```

Follow the instructions for updating your firmware in the *IBM 3582 Ultrium Tape Library Setup, Operator, and Service Guide*, GA32-0548.

10622
A.

7

IBM TotalStorage Ultrium Scalable Tape Library 3583

The fourth member of the IBM Ultrium family is the IBM TotalStorage Ultrium Scalable Tape Library 3583, shown in Figure 7-1 on page 130. It is a high-performance, reliable, scalable tape subsystem. Designed for tape automation, the IBM TotalStorage Ultrium Scalable Tape Library 3583 (IBM 3583) can be attached to iSeries, pSeries, xSeries, AS/400, RS/6000, Netfinity, and non-IBM servers, workstations, and personal computers that support SCSI HVD, SCSI LVD, and Fibre Channel interfaces. It uses IBM Ultrium tape drives for fast data transfer and reliability in automated library service. Each aspect of the library subsystem has been optimized for repeated, reliable unattended tape handling.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1325
Doc. 3698

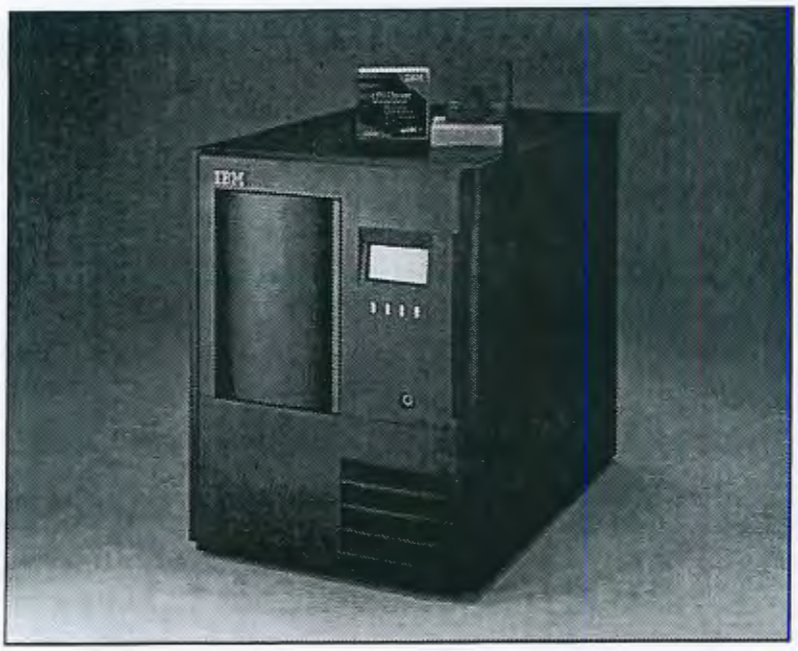


Figure 7-1 IBM TotalStorage Ultrium Scalable Tape Library 3583

The IBM 3583 tape library houses from one to six IBM Ultrium tape drives, which can have a native data transfer rate of up to 35 MBps and a cartridge capacity of up to 200 GB, depending on whether it is an Ultrium 1 or Ultrium 2 drive. Any combination of Ultrium 1 or Ultrium 2 drives may be installed. The drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm, which provides an effective data rate of up to 70 MBps and a cartridge capacity of up to 400 GB (with 2:1 compression) on IBM Ultrium 2 200 GB media. Multiple-drive models provide additional enhanced functions such as fast transfer of data, simultaneous backup, concurrent read-write operations, Control Path Failover, and fault tolerance. The Multi-Path Architecture enables a single library to be shared by multiple homogeneous or heterogeneous applications.

The IBM 3583 models feature cartridge capacities of 18, 36, and 72 cartridges; that is, capacities of 3.2 TB, 7.2 TB, and 14.4 TB of uncompressed Ultrium 2 data. With compression (assuming 2:1), the largest model of the 3583, the Model L72, can store 28.8 TB of Ultrium 2 data.

The IBM TotalStorage Ultrium Scalable Tape Library 3583 is an excellent choice if your application is experiencing growth in online storage requirements and you are considering a tape automation solution for your data storage needs.

10620
A-

7.1 Model description

The IBM 3583 supports up to six IBM LTO Ultrium tape drives. It comes standard with remote library management, multi-path architecture, and the ability to partition the library into three logical libraries. The library can be configured as a stand-alone unit or can be mounted in an industry-standard 19-inch rack. Additional optional features include Control Path Failover for AIX. The Library 3583 comes in three different models. The major difference between the models is the number of storage cells shipped with the initial order:

- *IBM 3583 Model L18* is supplied with space for 18 cartridges.
- *IBM 3583 Model L36* is supplied with space for 36 cartridges.
- *IBM 3583 Model L72* is supplied with space for 72 cartridges.

The models are summarized in Table 7-1:

Table 7-1 IBM 3583 model summary

Model	Cartridge Slots	Native Data Capacity with Ultrium 1	Native Data Capacity with Ultrium 2	IBM Ultrium Tape Drives
L18	18[a]	1.8 TB	3.6 TB	1-6
L36	36[b]	3.6 TB	7.2 TB	1-6
L72	72[c]	7.2 TB	14.4 TB	1-6

a. Plus one I/O Station slot
b. Plus one I/O Station slot
c. Including twelve I/O Station slots

The model numbering is an indication of how many cartridge slots the model was originally shipped with. However, all of the IBM 3583 models are the same physical size, and the two smaller models, L18 and L36, can be field-upgraded to hold up to 72 cartridges by the addition of upgrade features. The effect of these upgrades is shown in Table 7-3 on page 142.

7.1.1 Tape drives

The IBM 3583 libraries support the IBM LTO Ultrium 2 tape drives as well as the Ultrium 1 tape drives. Both types of tape drives and cartridges can be resident in the same 3583 frame. It is mandatory to have at least one IBM Ultrium drive installed in any of the libraries. Up to five more drives may be added either on the initial order or as field upgrades.

The installed drives may be any mixture of LVD, HVD, or 2 Gbps switched fabric Fibre Channel attached up to a total of six. However, LVD, and HVD interfaces

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1326
3698
Doc.

cannot be connected on the same SCSI bus. The drives are ordered for plant or field installation using chargeable feature codes:

- Feature #8003 provides one IBM Ultrium 1 tape drive with a Low Voltage Differential (LVD) Ultra2/Wide SCSI adapter.
- Feature #8004 provides one IBM Ultrium 1 tape drive with a High Voltage Differential (HVD) Ultra/Wide SCSI adapter.
- Feature #8103 provides one IBM Ultrium 2 tape drive with a Low Voltage Differential (LVD) Ultra160 SCSI interface.
- Feature #8104 provides one IBM Ultrium 2 tape drive with a High Voltage Differential (HVD) Ultra/Wide SCSI interface.
- Feature #8105 provides one IBM Ultrium 2 tape drive with a Fibre Channel Interface.

Each IBM Ultrium tape drive contains the electronics and logic for reading and writing of data, control of the tape drive, management of the data buffer, and error recovery procedures. All tape drives are packaged as a common assembly that is a Field Replaceable Unit (FRU), designed for quick removal and replacement. The cartridge capacities are unaffected by the number of drives installed.

7.1.2 Cartridge storage

As well as the installed tape drives, the library enclosure contains cartridge storage slots that are arranged in columns (from one to three depending on the library model). Each of the three storage columns has provision for an additional fixed slot located at the top of each column. This slot is reserved for future use.

The tape cartridges are stored in removable magazines, which are installed into the columns in the library (three magazines to each column). The magazines are designed so that tape cartridges can only be inserted in the proper orientation. Once inserted, the tape cartridges will be retained in the magazine so that they remain in place even when the magazine is inverted and shaken lightly. The magazines can only be inserted one way into the mounting columns in the library.

7.1.3 Barcode reader

A barcode reader is provided as standard with all IBM 3583 models, and it does not affect the slot capacity of the libraries. The barcode reader is used during the inventory process to locate all cartridges inserted in the library. This action is repeated every time the front door is opened to ensure that the inventory is updated, should a cartridge have been manually added, moved, or removed while the door was open.

7.1.4 I/O station

This facility allows the insertion and ejection of cartridges without interrupting the normal operation of the library. There are two types of I/O station:

- The single-cartridge station, where the cartridge can be inserted or ejected by opening the I/O station door
- The 12-cartridge station, where 12 cartridges are contained in two removable magazines that can be inserted or ejected by opening the I/O station door

Models L18 and L36 have the single-cartridge I/O station for tape cartridges and can be upgraded to a 12-cartridge station by the feature #8012. The model L72 has the 12-cartridge station installed as standard equipment.

7.1.5 Robotic system

In conjunction with the library control microcode, the robotic system identifies and moves cartridges between the storage slots, tape drives, and the I/O station. It has a number of components:

- A cartridge picker for placing cartridges in storage slots, tape drives, or the I/O station
- A barcode reader used to set up the library initially when it identifies the types of storage arrays and tape drives installed in the library, and in normal operation for reading the external labels on the cartridges, when it locates and categorizes all cartridges installed in the library
- A picker assembly for mounting the cartridge picker and the bar code scanner
- Y-axis and Z-axis drive motors for rotating the picker assembly, and moving it vertically, inside the library enclosure

7.1.6 Library control and operation

The library control unit contains the electronics and logic for autochanger operations. It controls all operations in the IBM 3583 libraries, including the interaction between the library and operators. The control unit Licensed Internal Code creates and maintains the library configuration, the physical location of the robotic system, and the inventory of cartridges. The database is kept in the flash memory of the library control hardware.

Requests issued from the server result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges to and from the tape drives and for inserting and ejecting cartridges. The host has records of the physical location of a cartridge in the library, and the physical location is also managed by the library.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1327
3698
Doc.

In addition to requesting movement of cartridges in the library, the host can obtain status, performance, configuration information, and information about the cartridges stored in the IBM 3583 tape library.

Each cartridge must have a machine- and operator-readable external barcode label to identify a media cartridge in the library during initial inventory and any time a cartridge is added to the library. The library stores the physical location of the cartridge in an inventory database based on the cartridge label. All host application requests for operations involving movement or use of a cartridge need only reference the physical location of the cartridge (using an element number as described in 7.11.3, "Element numbers" on page 150) for the library to perform the request.

7.1.7 Operator panel

An LCD operator control panel on the front of the machine provides status information and menu options. From this panel the operator can initiate actions such as moving and loading tape cartridges or invoking diagnostics.

7.1.8 Remote Management Unit

The Remote Management Unit (RMU) feature provides connectivity to Ethernet 10/100 LAN systems including Simple Network Management Protocol (SNMP). It allows library control, and configuration from authorized network attached consoles via a Web browser.

7.1.9 Library partitioning

The IBM 3583 library multi-path architecture (see 2.6, "Multi-path architecture" on page 46 for more information) allows homogeneous or heterogeneous open systems hosts to share the library's robotics without storage management middleware or a dedicated server acting as a library manager.

The library can be partitioned into as many as three logical libraries in order to share the library between different software platforms and applications (such as Windows 2000 and UNIX). Partitioning in this way means that they are able to share the library robotics independently of each other. Each logical library has its own distinct drives, cartridge storage slots, and control paths. If the application supports it, both Ultrium 1 and Ultrium 2 drives and media are allowed in the same logical library. Cartridges under library control are not shared between logical libraries, nor allowed to be moved between logical libraries. Input/output (I/O) slots are shared on a first-come-first-served basis.

For more information about the multi-path and partitioning capabilities of the IBM 3583 tape library refer to the library partitioning sections in these Redbooks:

- *Using IBM LTO Ultrium with Open Systems*, SG24-6502
- *Implementing IBM LTO in Linux and Windows*, SG24-6268

7.1.10 Multiple control paths

In addition to creating multiple logical libraries, you can also configure any logical library to have more than one control path. When you configure additional control paths, additional library sharing configurations and availability options are made possible. Access to the logical library is on a first-come, first-served basis, and each control path for a logical library can accept commands while the library is in use by another control path. By default, each logical library control path is available to servers through logical unit number 1 (LUN 1) of the first drive that is defined within that logical library.

Note: A logical unit number (LUN) is a number used by a server to identify a drive. The LUN for the Sequential Access device is always LUN 0 of the drive, and the LUN for the Medium Changer device is always LUN 1. All other LUNs are invalid addresses.

The IBM 3583 offers an optional control path failover feature that enables the host device driver to resend the command to an alternate control path; for example, to LUN 1 of the second drive in the same logical library. With control path failover installed, the alternate control path can include another HBA, SAN, or library control path drive. The device driver initiates error recovery and continues the operation on the alternate control path without interrupting the application. Only AIX hosts are currently supported for this feature.

7.1.11 SAN Data Gateway Module

The SAN Data Gateway Module (feature #8005) functions as an interface between LVD SCSI Ultrium 1 tape drives (#8003) in the library and Fibre Channel devices on the SAN. It provides attachment support for Fibre Channel interfaces using a Shortwave Gigabit Interface Convertor (GBIC) with SC connectors. The SAN Data Gateway Module is manageable over the IP network. It has an Ethernet 10/100 interface with an RJ-45 connector.

7.1.12 Maintenance

The cartridge storage slots, cartridge picker, and tape drives are accessed for maintenance purposes by opening the front door of the library. The tape drives,

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1328
3698

power supplies, and host interface board are accessed from the back of the library for maintenance.

7.2 Feature codes

The IBM 3583 can be ordered and/or upgraded with the feature codes in Table 7-2. We have not included cabling options; refer to the product publications for detailed information about configuring and ordering the IBM 3583.

Table 7-2 IBM 3583 feature codes

Feature	Description	Comment
1450	Multi-Path - Field Specify	Field only
1660	RMU/StorWatch™ Specialist	Field only
1680	Control Path Failover for AIX	Automatic control path failover to a pre-configured redundant control path in the event of the loss of a host adapter or control path drive, without aborting the current job in progress
8001	IBM LTO Ultrium 100 GB Data Cartridge	Plant only, see Media section for details.
8002	IBM Ultrium Cleaning Cartridge	Plant only, see Media section for details.
8003	LTO Ultrium 1 LVD Drive Sled	
8004	LTO Ultrium 1 HVD Drive Sled	
8005	SAN Data Gateway Module	Attachment support for Fibre Channel interfaces using a Shortwave 2 GBps Gigabit Interface Convertor (GBIC) with SC connectors. LVD SCSI attachment is via a VHDCI connector.
8006	Rack mount option	
~~8007~~	~~18-slot Tape Storage Column~~	~~Adds 18 slots~~ Maximum: - Model L18: two - Model L36: one
8008	Redundant power module	Redundant DC power module

Feature	Description	Comment
8010	20-pack of IBM LTO Ultrium 100 GB Data Cartridges	
8012	12-cartridge I/O station	Adds 18 slots in the door (12 of them can be used for non-disruptive exchange of cartridges) Maximum: - for L18 and L32: one - standard on L72
8013	6-cartridge magazine	Plant only
8101	IBM LTO Ultrium 200 GB Data Cartridge	Plant only, see Media section for details.
8103	LTO Ultrium 2 LVD Drive Sled	
8104	LTO Ultrium 2 HVD Drive Sled	
8105	LTO Ultrium 2 Fibre Drive Sled	
8110	20-pack of IBM LTO Ultrium 200 GB Data Cartridges	Plant only, see Media section for details.
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9215	Attached to Linux System	
9400	Attached to AS/400	
9450	Multi-Path - Plant Specify	Plant only
9600	Attached to AIX	

7.3 Physical attachments

In each of the different IBM 3583 tape library models, the interface (LVD, HVD, or Fibre Channel) on each of the drives is chosen by selecting the appropriate drive type (indicated by feature code numbers: #8003 for an LVD Ultrium 1 drive, #8004 for an HVD Ultrium 1 drive, #8103 for an LVD Ultrium 2 drive, #8104 for an HVD Ultrium 2 drive, and #8105 for a FC Ultrium 2 drive).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1329
3698
Doc

The IBM 3583 tape library can be attached to the iSeries, pSeries, xSeries, AS/400, RS/6000, RS/6000 SP systems, Netfinity and non-IBM servers, workstations, and personal computers that support the Ultra/Wide SCSI HVD, Ultra2/Wide SCSI LVD, and Fibre Channel interface.

SCSI or FC cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code should also be specified.

The IBM 3583 may be compatible with other servers, operating systems, and adapters. Contact your local IBM representative for a current list of supported configurations. You may also refer to the Interoperability Matrix (List of Supported Servers) on this Web site:

`http://www.storage.ibm.com/tape/lto/3583/3583opn.pdf`

Another resource is the IBM SSG HBA & SAN Interoperability Matrix on:

`http://ssddom02.storage.ibm.com/hba/hba_support.pdf`

7.4 Cabling

Cables are required to attach tape drives in the IBM 3583 to each server connection (up to the number of tape drives installed).

An interposer also may be required for attachment to various server adapters. One or more of the following Fibre Channel or SCSI cables should be specified on the IBM 3583.

7.4.1 Fibre Channel cables

A Fibre Channel cable is required to attach an IBM 3583 with the San Data Gateway Module feature (#8005) or the Fibre Drive feature (#8105) to host Fibre Channel adapters, switches, or other Fibre Channel components. The short-wave, multimode GBICs that are installed in the San Data Gateway Module are SC Duplex connectors.

Note: When feature #8005 is ordered as a plant feature, one of the no-charge features #9706 (5 m SC-SC Fibre Channel cable) or #9707 (7 m LC-SC Fibre Channel cable) can be selected to provide the fiber optic cable needed to connect to the host Fibre Channel adapter. When feature #8005 is ordered as an MES feature, one of the cables listed below should be ordered if needed.

The IBM LTO Ultrium 2 Fibre Tape Drive (#8105) comes with an LC Duplex connector. One 2 m LC-LC Fibre Channel drive-to-patch panel cable is included with each Fibre Drive feature (#8105).

Additional FC cables are available as optional features on the IBM 3583 for Fibre Channel attachment to host Fibre Channel adapters, Fibre Channel switches, or other Fibre Channel components:

- Feature #5907 - 7 m SC-LC Fibre Channel Cable
- Feature #5913 - 13 m SC-LC Fibre Channel Cable
- Feature #5922 - 22 m SC-LC Fibre Channel Cable
- Feature #5961 - 61 m SC-LC Fibre Channel Cable
- Feature #6005 - 5 m LC-LC Fibre Channel Cable
- Feature #6013 - 13 m LC-LC Fibre Channel Cable
- Feature #6025 - 25 m LC-LC Fibre Channel Cable
- Feature #6061 - 61 m LC-LC Fibre Channel Cable

7.4.2 SCSI cables

A host-to-library SCSI cable is available as no-charge feature #9704 or #9705 only with the initial IBM 3583 order. One of these cables is supplied with each library ordered. Features #9704 and #9705 cannot be ordered later as an MES; however, the same cables can be ordered after installation as chargeable MES upgrades by using feature codes #5305 and #5604. Feature #9704 supplies a 4.5 m SCSI cable with an HD68 connector at one end and a VHDCI connector at the other end; feature #9705 supplies a 5 m SCSI cable with HD68 connectors at each end.

Additional SCSI cables are available as optional features for LVD and HVD attachment to host adapters. These cables have HD68 connectors on both ends:

- Feature #5302, 2.5 m (8.2 feet) SCSI cable
- Feature #5303, 0.7 m (2.3 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The following cables differ in that they have a VHDCI connector at one end:

- Feature #5602, 2.5 m (8.2 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 25 m (82 feet) SCSI cable

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1330
Doc: 3698

One SCSI differential terminator and 0.5 meter drive-to-drive cable is included with each SCSI drive feature (#8003, #8004, #8103 and #8104).

7.4.3 Interposers

An interposer is required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries and AS/400 to adapter #6501.
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable. This interposer (a 0.3 m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

7.4.4 Terminator

An inline terminator is required when attaching the 3583 library to Hewlett-Packard V-Class systems with adapter A4800A.

The following inline terminator is available:

- Feature #5098, Inline HVD SCSI Terminator

7.4.5 Cable length limitations

The native Fibre Channel drive and the San Data Gateway Module are capable of 2 Gbps speed. They automatically switch to a 1 Gbps speed if they are attached to a 1 Gbps host Fibre Channel adapter, switch, or other Fibre Channel components. With 1 Gbps speed the maximum cable length is limited to 300 m (984 feet), and with 1 Gbps speed to 500 m (1640 feet).

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection (for example, one host connected to only one tape drive). If using multi-drop interconnection (such as one host connected to more than one tape drive on the same SCSI bus), then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using point-to-point or multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

10610
A.

7.5 Upgrades and optional features

You can add MES features to each model type in the IBM 3583 family in order to add capacity in terms of drives and cartridge cells, and to add the 12-cartridge I/O station. This effectively takes the place of model upgrades as there are no upgrades available for the IBM 3583 series.

In other words, you cannot upgrade an IBM 3583-L18 to an IBM 3583-L36 or L72. Similarly, an IBM 3583-L36 cannot be upgraded to an IBM 3583-L72.

7.5.1 Upgrade features

You can expand any IBM 3583 model to the maximum capacity of the largest model (L72) with the addition of MES features.

Adding drives:
You can add IBM LTO Ultrium drives to any library model to a maximum of six drives in total. The drives may be LVD, HVD, or Fibre in any combination. To install an LVD drive, add feature #8003 (Ultrium 1) or #8103 (Ultrium 2), to add an HVD drive, add #8004 (Ultrium 1) or #8104 (Ultrium 2), and to add a Fibre drive, add #8105 (Ultrium 2).

Adding cartridge capacity:
You can add an additional 18 tape cartridge slots to either of the smaller IBM 3583 models using feature #8007. You can add one or two of these features to model L18 (for a total of 36 or 54 cartridge slots), and you can add one feature to model L36 (for a total of 54 cartridge slots).

You can install a 12-cartridge I/O station to models L18 and L36 by adding feature #8012. This feature accommodates the 12 cartridges in two six-slot cartridge magazines that are accessed by opening the I/O station door. In addition to the two magazines, this feature supplies six additional fixed slots in the library door for a total of 18 additional slots. This feature in combination with feature #8007 provides the maximum slot capacity and function for the two smaller IBM 3583 models.

Table 7-3 on page 142 shows how to upgrade the capacity of 3583-L18 and 3583-L36 libraries by adding extra 18-slot tape storage columns (feature #8007) and by adding the 12-cartridge I/O station (feature #8012). You may choose to set up the12-cartridge I/O station as storage slots or I/O slots.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1331
3698
Doc.

Table 7-3 IBM 3583 capacity upgrades

3583 model	Extra tape storage columns	Single cartridge I/O station	12 cartridge I/O station defined as storage	12 cartridge I/O station defined as I/O
L18	0	18 storage 1 I/O	36 storage 0 I/O	24 storage 12 I/O
L18	1	36 storage 1 I/O	54 storage 0 I/O	42 storage 12 I/O
L18	2	54 storage 1 I/O	72 storage 0 I/O	60 storage 12 I/O
L36	0	36 storage 1 I/O	54 storage 0 I/O	42 storage 12 I/O
L36	1	54 storage 1 I/O	72 storage 0 I/O	60 storage 12 I/O
L72	Not available	not available	72 storage 0 I/O	60 storage 12 I/O

7.5.2 Optional features

Two optional features are available:

- Feature #8006, rack mount option
  The IBM 3583 libraries can be installed either stand-alone or in a standard EIA 19-inch rack. They occupy the full width of the rack and require 14 units of rack space (24.5 in or 62.2 cm). This is the chargeable feature that provides the necessary hardware to mount the library in the rack.
- Feature #8008, redundant power module
  This chargeable feature supplies a redundant DC power module for customers requiring an extra level of back-up protection. You can order one of these features per library.

7.6 Environmental specifications

The IBM 3583 Scalable is a stand-alone, medium-sized library unit that can be placed on a desk or the floor.

IBM 3583 models have from one to six drives and up to 72 cartridge slots. The physical dimensions are:

- Width: 48.1 cm (18.9 in)
- Depth: 73.5 cm (28.9 in)

10608
A-

- Height: 68.5 cm (27.0 in) for a stand-alone library on casters
- Maximum weight: 116.6 kg (257 lb) with six drives and 72 cartridges

7.7 Host platforms and device drivers

The following no-charge specify codes indicate the server platform to which the IBM 3583 is attached:

- Feature #9210, attached to HP-UX
- Feature #9211, attached to Sun system
- Feature #9212, attached to Windows NT system
- Feature #9213, attached to other non-IBM system
- Feature #9215, attached to Linux system (Model L23 and H23)
- Feature #9400, attached to iSeries system
- Feature #9600, attached to RS/6000 system

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3583). Sometimes the driver code is supplied as part of the operating system code (for example, in OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

Ultrium 1

The IBM 3583 is shipped with the device drivers to support Ultrium 1 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.2 or later
- Sun Solaris 2.6, 7, and 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- HP-UX 11.0
- OS/400 V4R4

Ultrium 2

The IBM 3583 is shipped with the device drivers to support Ultrium 2 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.3 or later
- Sun Solaris 7, 8, 9
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- Windows 2003
- HP-UX 11.0, 11.i

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1332
Doc. 3698

- OS/400 V5R1 or later
- Linux distributions: Linux Red Hat 7.2 32-bit and 64 bit Kernels, Linux Red Hat 7.3, Red Hat Advanced Server 2.1, SuSE Linux Enterprise Server Update

Tip: The device driver CD or diskette that is shipped with the IBM 3583 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

7.7.1 Device driver installation

Install the IBM device drivers for the IBM 3583 as follows:

- If you intend to use the IBM 3583 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3583.
- If you do not intend to use the IBM 3583 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide*, GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3583 with a commercial software application, IBM recommends that you install any IBM-supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples of using the Ultrium drives are given in the redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

7.8 Storage applications

The software to manage the IBM 3583 is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software vendors. A list of compatible software is available at:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1 and Ultrium 2 support, and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more detailed information of specific versions and platforms supported.

7.9 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each library order[1]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3583:

- Feature #8001 provides a single 100 GB Ultrium data cartridge. It is a chargeable feature, and a maximum of 19 can be ordered.
- Feature #8002 provides a single Ultrium cleaning cartridge. It is a chargeable feature and a maximum of three can be ordered.
- Feature #8010 provides a pack of twenty 100 GB Ultrium data cartridges. It is a chargeable feature, and the maximum of one can be ordered.
- Feature #8101 provides a single 200 GB Ultrium 2 Data Cartridge. Up to 19 can be ordered. The cartridges come with a barcode label but it is not affixed.
- Feature #8110 provides a pack of twenty 200 GB Ultrium Data Cartridges with unattached barcodes labels. It is a chargeable feature, and a maximum of four can be ordered.

Note: All of the media features are available only with the initial order. They cannot be ordered as an MES feature. After the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about ordering supplies and cartridges, with or without labels.

7.10 Installation and performance considerations

iSeries configurators allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape library on an input/output port may affect drive performance.

Installing more than one Ultrium drive on a SCSI bus may affect tape drive performance. For optimal performance, it is recommended that no more than one IBM Ultrium drive be attached to an individual SCSI bus.

[1] All media and cleaning cartridges are warranted separately from the IBM TotalStorage Ultrium Scalable Tape Library 3583.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1333
3698
Doc.

Intermixing of other SCSI devices on the same SCSI bus as the IBM 3583 may affect performance of those devices.

While the IBM Ultrium tape drives provide the capability for high tape performance, other components of the system may limit the actual performance achieved. The compression technology used in the tape drive can typically double the amount of data that can be stored on the media; however, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

The weight of the IBM 3583, depending on the number of drives and cartridges, may be up to 257 lbs (116.6 kg). If more than one library is mounted in a rack, a tipping hazard could be created. Customers are advised to take necessary safety precautions when mounting the libraries in the racks.

7.11 IBM 3583 initial set-up

The following section covers some of the major items required to implement, manage, and operate the IBM 3583. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

7.11.1 SCSI ID and LUN assignment

The SCSI ID and LUN assignment in the IBM 3583 tape library depends on whether the multi-path feature is installed.

If the multi-path feature is installed, the Logical Unit Number (LUN) for the tape drive is always LUN 0, and the LUN for the Medium Changer device is always LUN 1. All other LUNs are invalid addresses.

Note: The Medium Changer SCSI ID is the same as the SCSI ID for the first drive. You can enable additional drives to optionally provide Medium Changer (LUN 1) addressing by configuring more than one logical library or by enabling additional control paths.

If the multi-path feature is not installed, the IBM 3583 tape library uses a separate SCSI device address for the robot so you will have to define a SCSI ID for the tape library unit. In this case the LUNs for both the library and the tapes are always LUN 0.

10604
A.

Note: Do not use SCSI ID *F* as it is reserved for internal use by the SCSI library. SCSI ID 7 is also often used by the host SCSI adapter.

The IBM 3583 consists of up to seven SCSI devices: the library and up to six drives. The default settings for the SCSI IDs are 6 for the library and 0 through 5 for the drives. Depending on your requirements, you may need to change the SCSI ID default settings for your installation.

The IBM 3583 is a SCSI target device and can be connected to a single-ended LVD or HVD SCSI bus. Both ends of the bus must be terminated and a terminator is shipped with each library. The design of an IBM 3583 enables the SCSI type (single-ended, LVD, or HVD) to be configured at the customer site via a switch located on the SCSI Interface PCBA. Although the IBM 3583 can be attached to a wide SCSI bus, it is not a wide SCSI device and its SCSI ID must be in the range of 0 to 7.

7.11.2 Identifying library locations

The convention shown in Table 7-4 is used to identify the coordinates of each library element (storage, slots, or drives).

Table 7-4 IBM 3583 storage slot coordinates

First digit	Second digit	Third digit
Column	Magazine	Row

The columns are numbered from 1 to 5 starting from the I/O station column and continuing clockwise (see Figure 7-2 on page 148).

RQS nº 03/2005 CN
CPMI - CORREIOS
Fl. Nº 1334
Doc. 3698

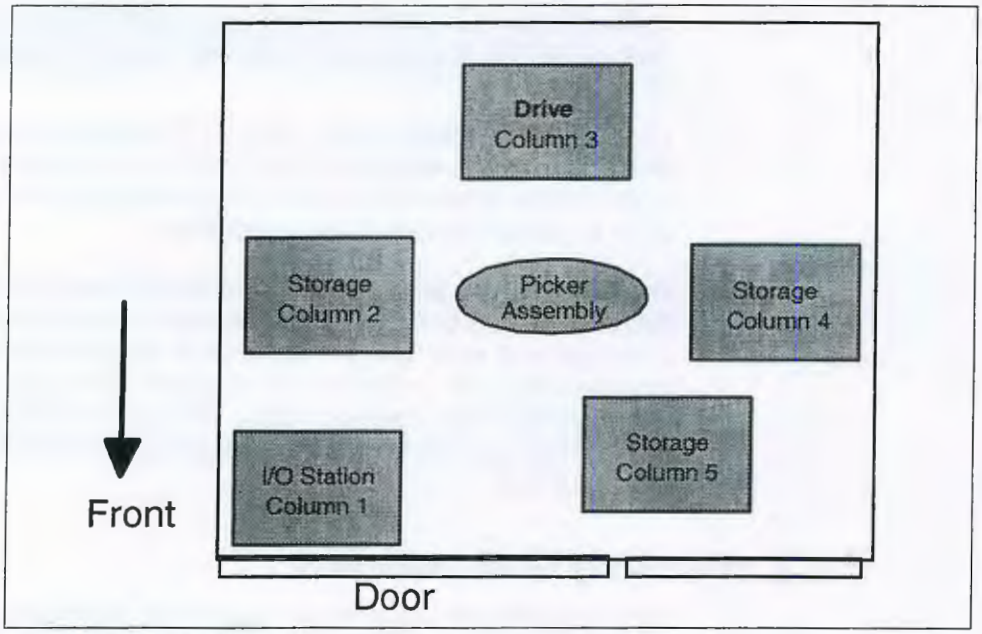


Figure 7-2 IBM 3583 storage columns: top view

The magazines within each column are designated A to C from top to bottom (label 1 in Figure 7-3 on page 149).

The rows within each magazine are numbered from 1 to 6 from top to bottom (label 2 in Figure 7-3 on page 149).

The drives within the drive column are designated from A to F from bottom to top (label 3 in Figure 7-3 on page 149).

The fixed slots in the storage columns (label 4 in Figure 7-3 on page 149) are reserved for future functions.

So, to illustrate this convention, consider the coordinates:

```
1-A-6
```

These coordinates would refer to the slot found in column 1, the top-most of the three magazines, and the bottom slot within that magazine.

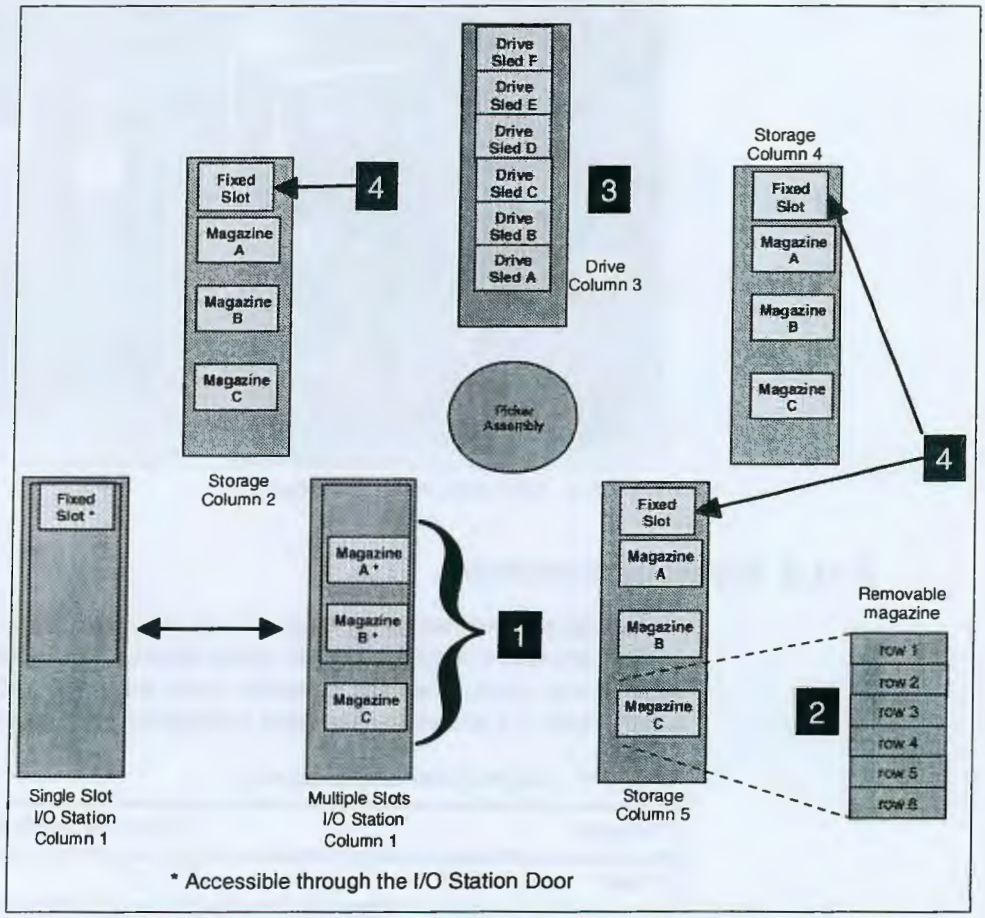


Figure 7-3 IBM 3583-L72 location logical view

Figure 7-4 on page 150 shows the actual picture of an IBM 3583 with a view of the front door opened showing I/O station column 1. This diagram also shows a good view of the 12-slot I/O station option.

Note: The only components accessible in a non-disruptive mode are the magazines located in the I/O station door (label 1 in Figure 7-4 on page 150).

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1335
Doc. 3698

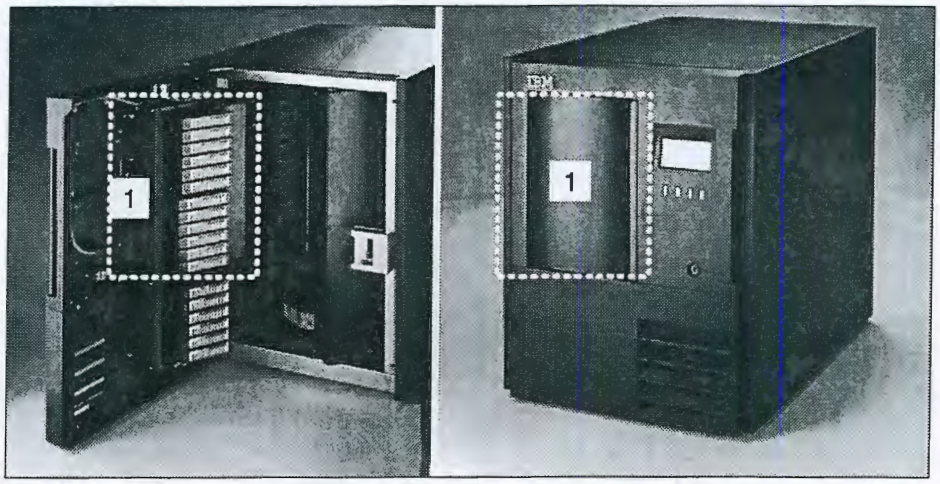


Figure 7-4 IBM 3583 front view, open door

7.11.3 Element numbers

To manipulate the media within the library, the host must reference each movement with source and target designations. This is done via element addressing, which specifies precisely which slots within the library are to be used. Table 7-5 shows the element addressing scheme used for the IBM 3583.

Table 7-5 IBM 3583 element numbering

Column	Element numbers
Picker	1h (1)
Single-Slot I/O Station	10h (16)
Multi-Slot I/O Station	10h - 1Bh (16 - 27)
Drives	100h - 105h (256 - 261)
Storage	1000h - 1047h (4096 - 4167)

Drives are addressed from bottom to top.

The I/O station is addressed from top to bottom. Storage slots are addressed from top to bottom, column by column.

7.12 Operator panel and RMU

Normally, the host issues commands to the IBM 3583 tape library. Operator control is provided via the Operator Panel or via the TotalStorage Specialist Web interface on the Remote Management Unit (RMU). The operator is responsible for:

- Starting the IBM 3583
- Shutting down the IBM 3583
- Handling media
- Updating firmware
- Cleaning drives

For detailed information about operator tasks refer to the *Operating Procedures* chapter in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

7.12.1 Operator panel

The operator panel provides communication between the operator and the IBM 3583. Visual indications and push buttons enable the operator to control the IBM 3583.

As shown in Figure 7-5 on page 152, the IBM 3583 operator panel is divided into six discrete areas:

- I/O Station status:
  The I/O Station status area provides constant information about the I/O Station (label 1 in Figure 7-5 on page 152). The information provided will state whether the I/O station is locked. The status of the I/O door and a physical representation of an occupied I/O station slot is indicated by a blacked-out area.
- Library status:
  The library status area displays informational status such as the library's online or offline status and the library reports status or messages to solicit operator intervention (label 2 in Figure 7-5 on page 152).
- Messages:
  The message area displays six lines of text, graphic representations, or a combination of both (label 3 in Figure 7-5 on page 152). Each text line can be up to 20 characters long. The display communicates interactive dialogs, special messages, alerts, and library configurations. More details are covered in Using the Operator Panel Menu in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1336
Doc. 3698

- Drive status:
  The drive status area (label 4 in Figure 7-5) provides constant information about the drives, such as:
  - Presence of tape drive (illustrated by a black outlined box for each drive)
  - Power to the tape drive
  - Cleaning requirements
  - Compression
  - Write protection
  - Tape activity
- Soft keys:
  The soft keys reference the push buttons located beneath which are used to perform commands displayed in the soft keys area and to move through the various displays of the operator panel (label 5 in Figure 7-5).
- Push buttons:
  The actual physical buttons that perform the commands referred to by the soft keys located above each one of them (label 6 in Figure 7-5).

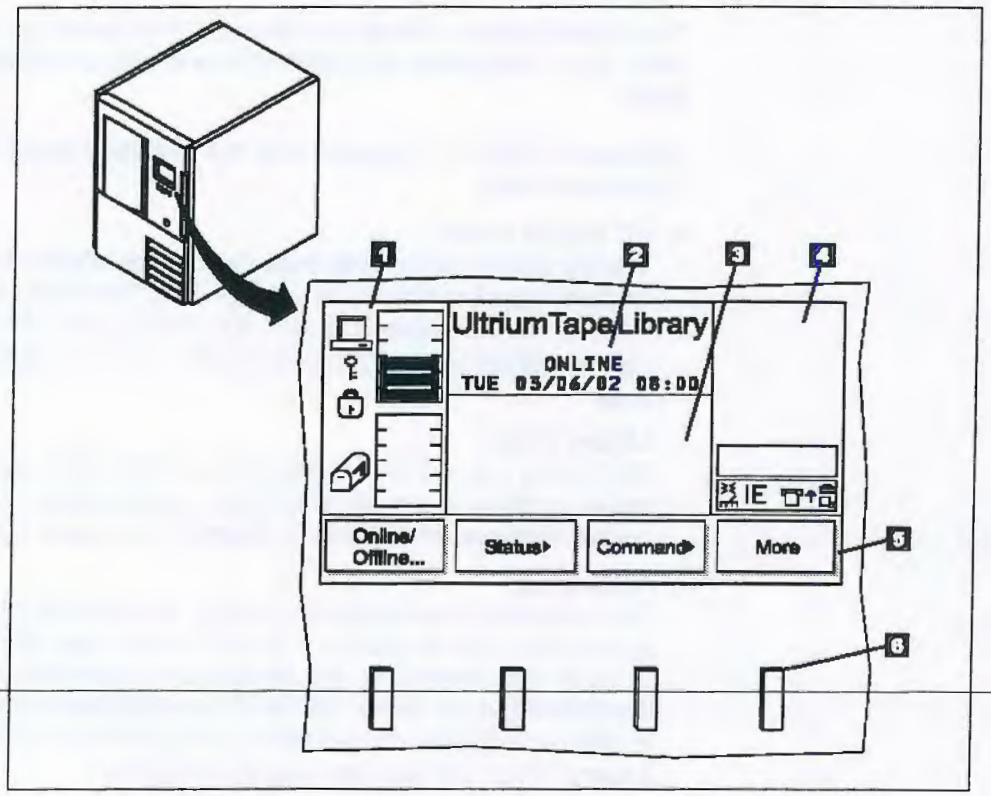


Figure 7-5 IBM 3583 tape library operator panel

10598
A-

Menu options

Each menu is accessible through the Operator Panel push buttons. Figure 7-6 shows the flowchart of the IBM 3583 library menu options. For more information about these functions refer to the Operating Procedures chapter in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

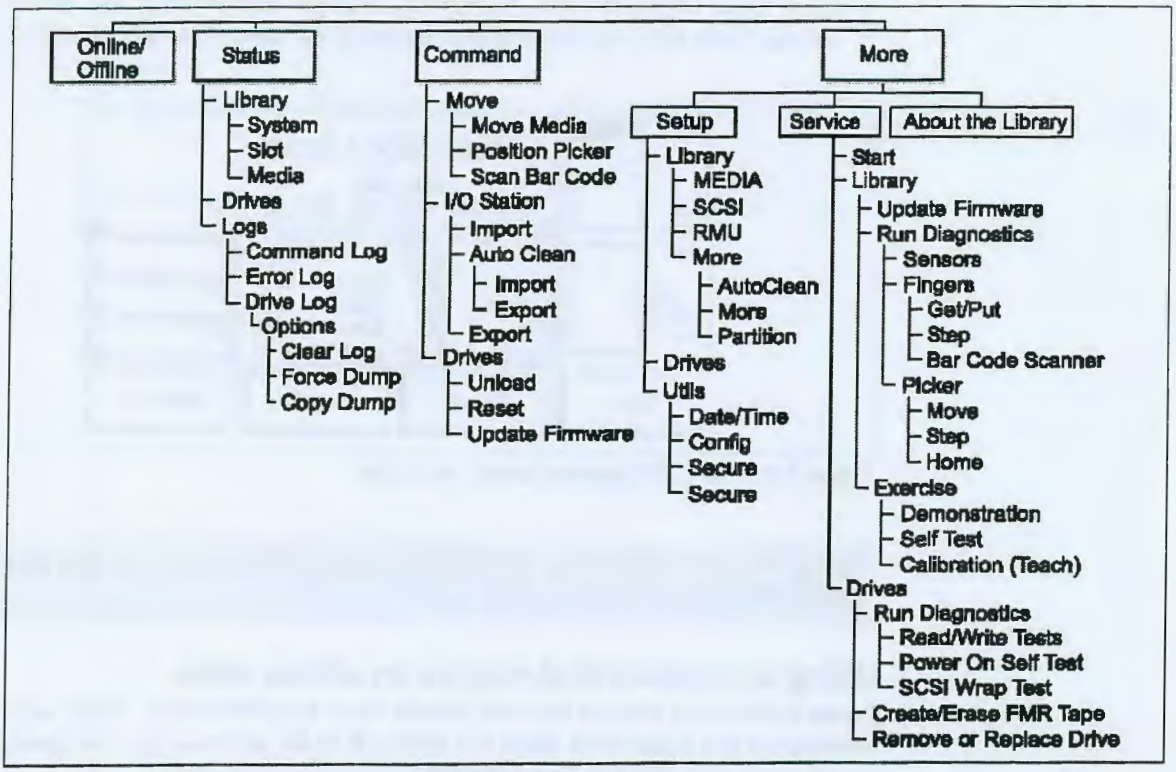


Figure 7-6 IBM 3583 flowchart of library functions

Menu guidelines

All of the the menus and their options are grouped according to function. As shown in Figure 7-7 on page 154, some options are followed by special characters, based on the following system:

- A keyword leading to another menu is suffixed by a small black arrow.
- A keyword leading to a dialog box is suffixed with three closely spaced dots.
- A keyword leading to an immediate action has no suffix.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1337
Doc 3698

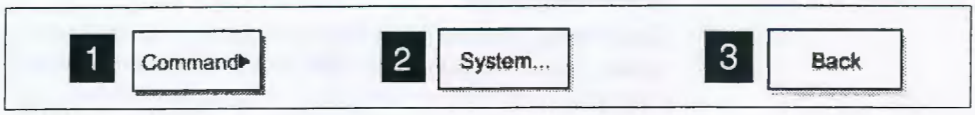


Figure 7-7 IBM 3583 soft key symbols

- Most fields on the menus, submenus, dialogs, and screens are read-only. Those fields that are writable are shown in reverse video (Figure 7-8).

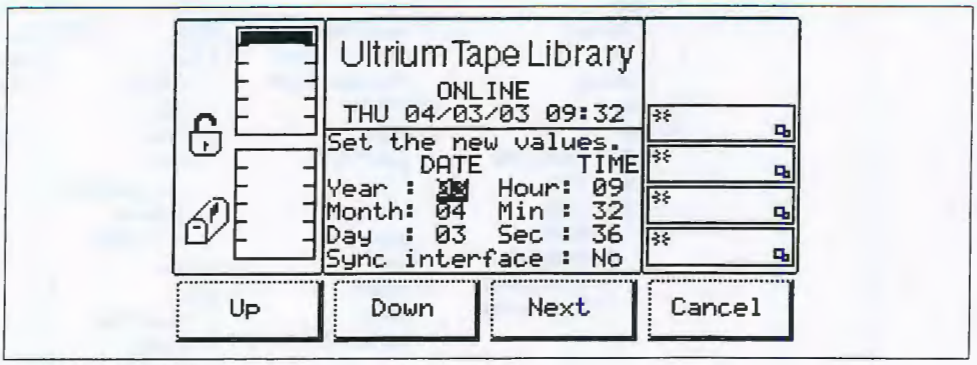


Figure 7-8 IBM 3583 operator panel: input field

Note: The information menus are not updated dynamically. To view changes, reselect the menu that was changed.

Using commands that require an offline state

Some commands require that the library be in an offline state. If any such commands are attempted while the library is in an online state, the operator will be requested to take the library offline.

Operator intervention message

If a problem causes an operator-intervention message to appear, refer to Operator Intervention Messages in the Error Messages appendix of the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

7.12.2 RMU with TotalStorage Specialist

The Remote Management Unit (RMU) provides remote access to the Ultrium Scalable Tape Library over a network. You can attach the library to the network through a 10/100 Ethernet port on the RMU. All available functions are accessible without the need of a dedicated server or separate software. You can access the library through any server on the network by entering the IP address

10596
A.

or IP name in a Web browser. The operator panel page of the TotalStorage Specialist Web interface is protected by a password and is a direct interface to the operator panel of the attached library.

As shown in Figure 7-9 on page 156, the IBM 3583 TotalStorage Specialist Web interface has three discrete frames:

- Left navigation:
  The left navigation frame (label 1 in Figure 7-9 on page 156) contains hyperlinks where you can log out the current user, display a brief description of the tabs from the center navigation frame, open the library's online documentation, download the SNMP MIB file, display contact information for technical support, and display the current version of the RMU firmware.
- Center navigation:
  The center navigation frame (label 2 in Figure 7-9 on page 156) has tab-style hyperlinks for Status information, Configuration, Firmware, Diagnostics file, Operator panel, and Logs. If you select a tab other than the Status tab, then you have to enter a logon name and password.
- Top information:
  The top information frame (label 3 in Figure 7-9 on page 156) contains information for you to identify the tape library that you are remotely managing. The frame shows the URL identifier and library type. The URL identifier is the hostname given to the library during initial configuration. The library type is the ID string of the library and is taken from standard inquiry data.

More details are covered in Operator Panel and RMU section in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1338
Doc. 3698

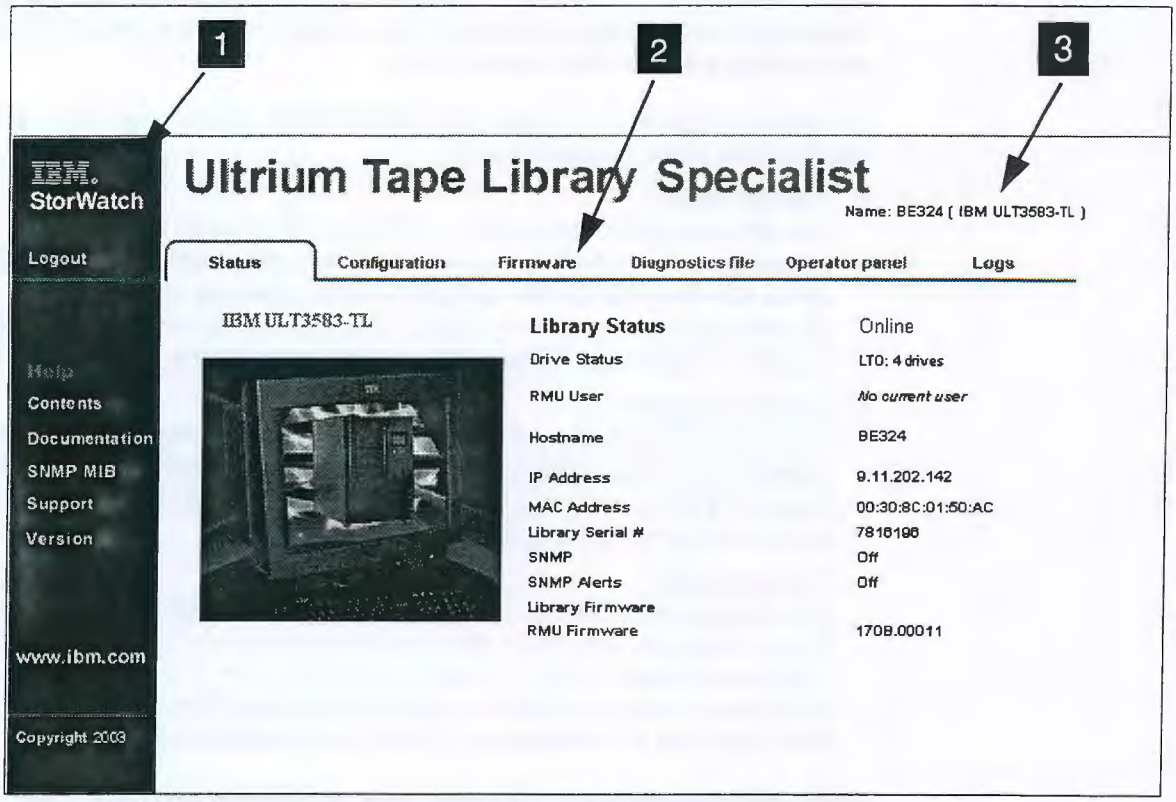


Figure 7-9 IBM 3583 TotalStorage Specialist Web interface

7.13 Random access

The library operates in random access mode, which means that you can access any cartridge in any sequence. This mode normally requires software that generates commands that are sent to the library. The server's application software manages the cartridges (and thus the data).

7.14 Drive cleaning

All of the IBM Ultrium Tape Drives have an integrated cleaning mechanism that brushes the head at load time and again when unloading a cartridge. Along with this, drives have a cleaning procedure using a special cleaning cartridge, should this become necessary.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

With each IBM 3583 tape library, a specially labeled IBM LTO Ultrium Cleaning Cartridge is supplied to clean the drive head. The drive determines when the head needs to be cleaned, and alerts you by displaying CT on the message display.

7.15 Firmware upgrades

Each IBM Ultrium tape drive and tape library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the current firmware is installed on your IBM LTO tape drives, library and RMU. As the IBM 3583 is designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed. Determine the latest level of firmware available from the Web site

`http://www-1.ibm.com/support/docview.wss?rs=547&context=STCVQ6Y&q=ssg1*&uid=ssg1S4000044&loc=en_US&cs=utf-8&lang=en+en`

Follow the instructions for updating your firmware in the *Operating Procedures* chapter in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411, or from

`http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_drivefw`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1339
Doc 3698

10593
A.

8

IBM TotalStorage UltraScalable Tape Library 3584

Designed for automated tape handling, the IBM TotalStorage UltraScalable Tape Library 3584 (IBM 3584) shown in Figure 8-1 on page 160 is the largest member of the IBM Ultrium family of tape library storage solutions. Each aspect of the subsystem is designed to optimize data access and reliability. IBM LTO Ultrium tape drives are compact, high-performance storage devices that support the operations required by today's network and e-business servers. The IBM 3584 supports IBM LTO Ultrium 1 and IBM Ultrium 2 drives.

The IBM TotalStorage UltraScalable Tape Library 3584 provides tape storage solutions for the large, unattended storage requirements from today's mid-range up to enterprise open systems environment. Combining reliable, automated tape handling and storage with reliable, high-performance IBM LTO Ultrium tape drives, the IBM 3584 offers outstanding retrieval performance with typical cartridge move times of less than three seconds.

The IBM 3584 can be partitioned into multiple logical libraries. This makes it an excellent choice for consolidating tape workloads from multiple heterogeneous open-system servers.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1340
3698
Doc.

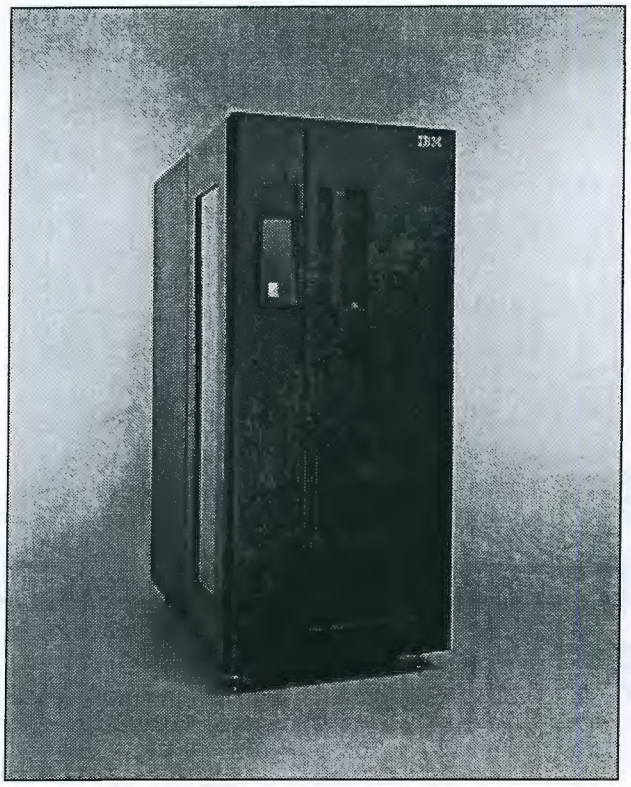


Figure 8-1 IBM 3584 UltraScalable tape library L32

The IBM 3584 is a modular tape library consisting of frames that house tape drives and cartridge storage slots. You can install a single-frame base library and add up to 15 additional frames, tailoring the library to match your system capacity and performance needs from 14 TB to 1376 TB (28 TB to 2752 TB with 2:1 compression), and using up to 192 IBM LTO Ultrium tape drives. The high granularity of the IBM 3584 library configurations, and its features and capacities are designed to match a wide variety of customer requirements.

The IBM 3584 is an excellent choice if you:

- Are experiencing rapid growth in online storage requirements
- Are considering tape autoloaders and tape libraries with software for automatic backup, archive, or fast-access tape operation to accommodate growth and reduce manual operations
- Have standardized on IBM LTO Ultrium format tape
- Are looking for an IBM LTO Ultrium tape solution requiring large cartridge capacity and fast data streaming transfer capability

10591
A

8.1 Model description

Two IBM 3584 frame models can be installed together to make up the library:

- *IBM 3584 Library Unit L32*, the base frame for the IBM 3584 library, which can be installed on its own or in combination with the model D32.
- *IBM 3584 Expansion Unit D32*, up to 15 of which can be installed with the model L32 base frame. Note that the capacity expansion feature on the L32 is required (either feature #1603 or #1653) before adding D32 frames.

An IBM 3584 library can consist of a single frame (which must be the L32 model), or multiple frames, up to 16 in total. You must install a model L32 before you can add model D32s to the library, and you cannot install more than one L32 in a single library.

Note: If you are familiar with the IBM TotalStorage Enterprise Automated Tape Library 3494, then you may see that the IBM 3584 has the same form factor and looks broadly similar. However, it is *not* the same frame or internal components as the IBM 3494. You cannot mix IBM 3584 and IBM 3494 frames in the same library assembly, as the two libraries function in completely different ways.

8.1.1 IBM 3584 Library Unit L32

The IBM 3584 Library Unit L32, shown in Figure 8-2 on page 162, can be installed on its own as a complete library enclosure, or it can have up to 15 expansion frames attached to it. This frame provides the major library components for the whole library, whether it has a single or multiple frames. It also provides cartridge storage capacity and tape drives. The D32 expansion frames must be added to the right of the L32 frame.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1341
Doc 3698

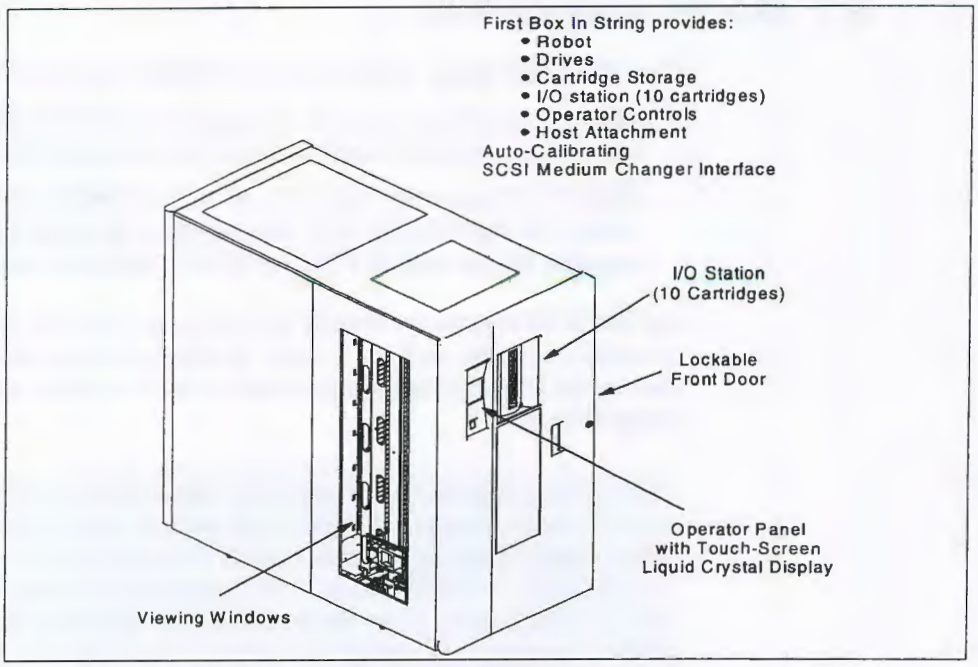


Figure 8-2 IBM 3584-L32 base frame view from front left

The number of cartridge storage slots ranges from 87 to 281, with the base frame standard of 141 slots, installed in the rear. Additional slots can be added on the door side for a maximum of 281 cartridge slots. The additional slots have to be enabled with the Capacity Expansion feature (FC #1603 or #1653), which enables use of the slots on the door. This gives a maximum data capacity for the L32 of 56 TB native (up to 112 TB with a 2:1 data compression) if you are using LTO 2 Technology. See 8.2.12, "Capacity" on page 181 for precise guidance on model L32 cartridge slot storage capacities.

At least one tape drive must be installed in the model L32 with the option to install 11 more drives for a maximum of 12 tape drives in the L32 frame. As you add drives, there is an incremental reduction in storage slots once you exceed four installed drives.

Each L32 has a standard 10-slot cartridge input/output station for importing or exporting cartridges from the library without requiring re-inventory or interruption of library operations. Optional features can provide 20 additional input/output slots. The lockable library door can be opened for bulk-loading IBM LTO Ultrium tape cartridges. Re-inventory of the cartridges is done in less than 60 seconds per frame each time the library door is closed. A barcode reader mounted on the autochanger scans the cartridge labels at less than one minute per frame. A door lock is included to restrict physical access to cartridges in the library.

10589
A-

8.1.2 IBM 3584 Expansion Unit D32

The IBM 3584 Expansion Unit D32, shown in Figure 8-3, cannot be installed without the L32 base frame, which must be the first frame in the library. The L32 frame also must have the capacity expansion feature (FC #1603 or #1653) installed as a prerequisite to install additional D32 frames. The D32 provides cartridge storage space and houses additional drives. Up to 15 expansion frames can be added to the L32 base frame.

When no drives are installed, the D32 has 440 installed cartridge storage slots. An L32 base frame and 15 D32 expansion frames with a minimal drive configuration provides a maximum capacity of 6881 storage slots with a total capacity of 1376 TB without compression using IBM Ultrium 2.

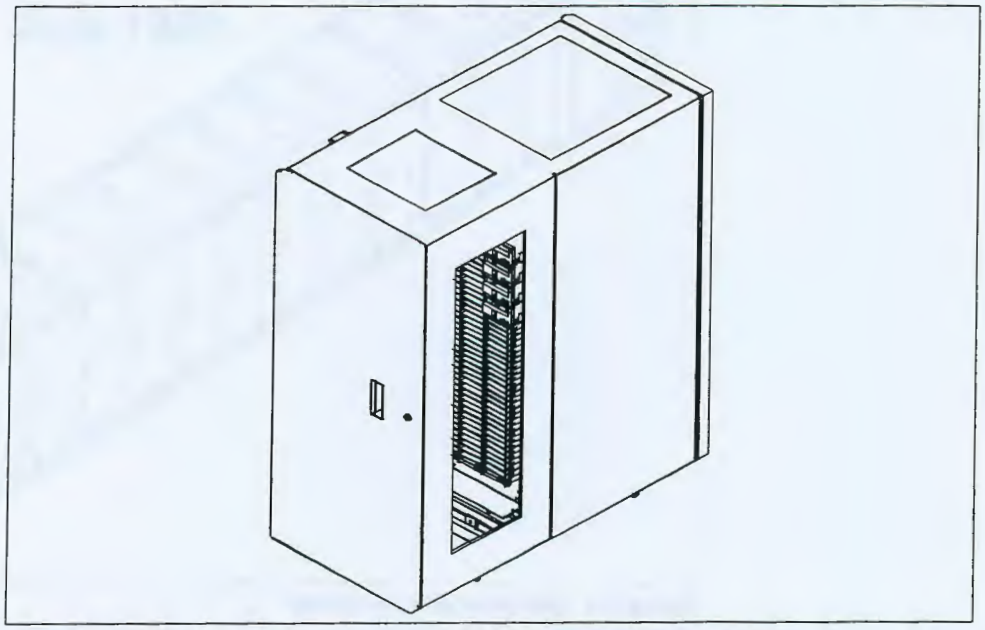


Figure 8-3 IBM 3584-D32 library expansion frame viewed from the right

Each IBM D32 houses up to 12 drives; the minimum number of installed drives is zero. In other words, you do not have to install tape drives in the model D32, but can use it solely to expand the number of storage slots in the library.

If one or more tape drives are installed in the D32 then the Frame Control Assembly Feature is also required (#1452). This feature provides the hardware and firmware required to support IBM LTO Ultrium drives within the D32, and also provides a redundant AC line feed for the L32 accessor.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1342
Doc. 3698

The base L32 is always on the left and as many as 15 additional D32 expansion frames can be added to the right side. During the installation of additional D32 frames, the x-rail of the L32 frame where the accessor resides will be extended, so that the accessor can move through the new installed frame.

A fully configured IBM 3584 with one L32 frame and 15 D32 frames (see Figure 8-4) supports up to 192 drives. As you add drives to each D32, there is an incremental reduction of storage slots for each set of four tape drives you install.

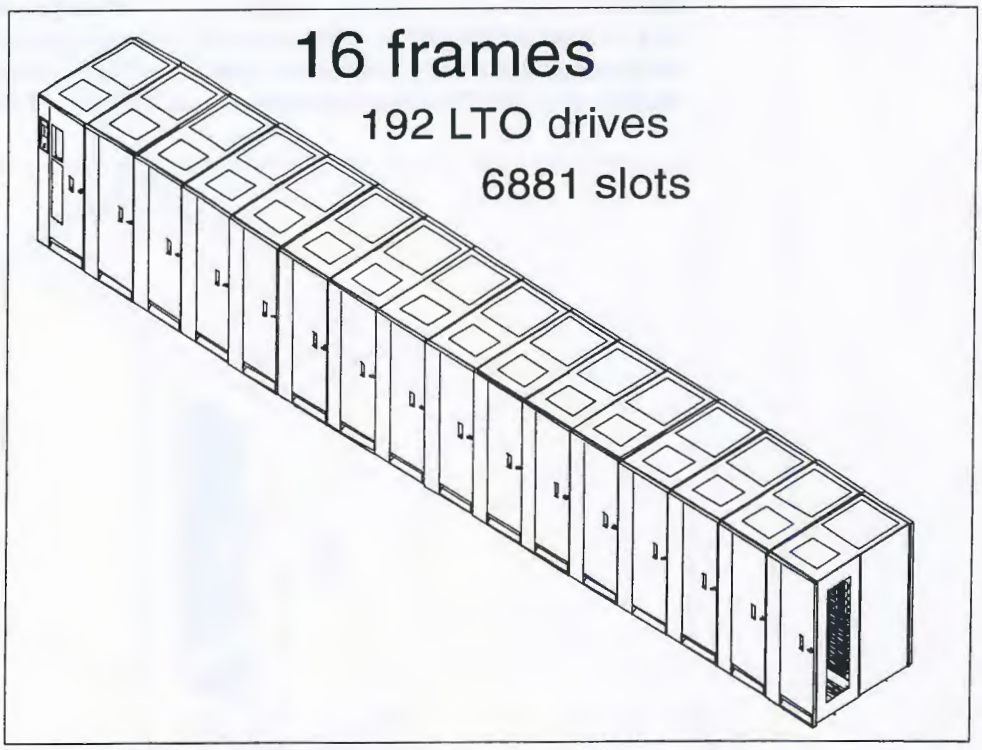


Figure 8-4 IBM 3584 with 16 frames

10587
A.

8.2 Library components

The major IBM 3584 library components are shown in Figure 8-5.

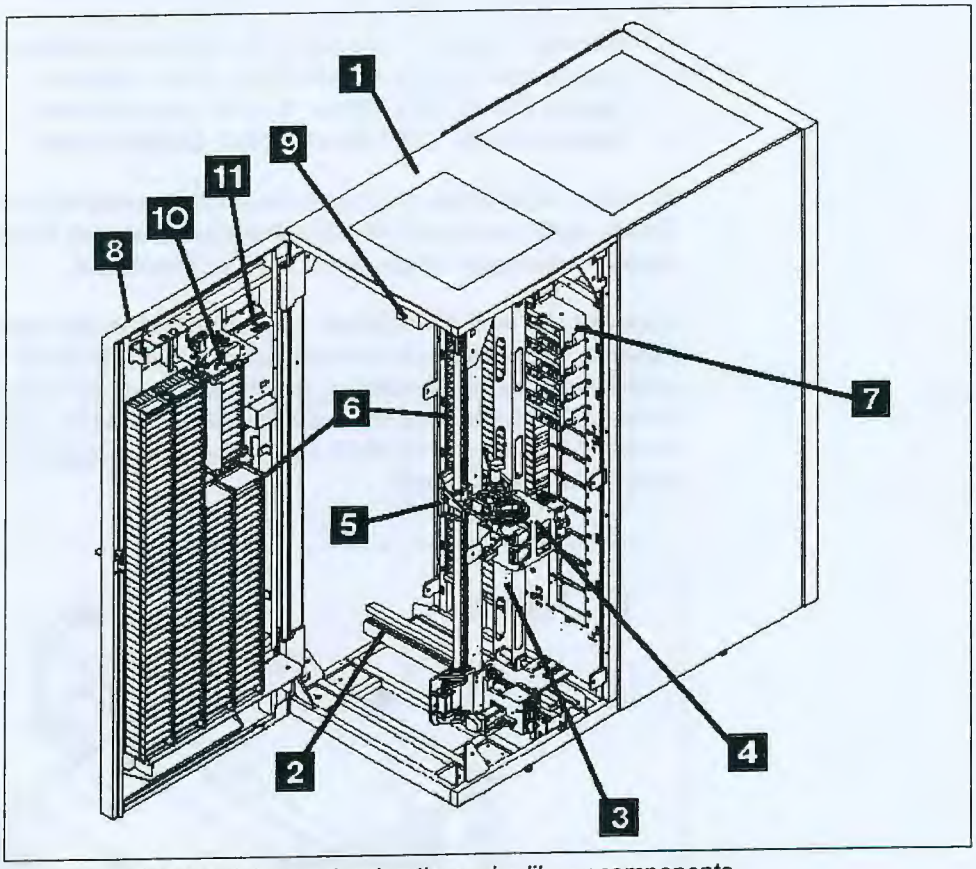


Figure 8-5 IBM 3584 library showing the major library components

1. *Library frame*
2. *x-Rail system*
3. *Cartridge accessor*
4. *Dual-gripper transport mechanism*
5. *Accessor controller*
6. *Cartridge storage slots*
7. *IBM LTO Ultrium drive*
8. *Front door*
9. *Door safety switch*
10. *I/O station*
11. *Operator panel and controller*

8.2.1 Tape drives

~~The IBM 3584 library houses IBM LTO Ultrium drives. Both Ultrium 1 and~~ Ultrium 2 drives may be installed in the same frame.

RQS nº 03/2005 CN
CPMI - CORREIOS
Fls Nº 1343
Doc 3698

IBM LTO Ultrium drives may be attached to a SCSI host system using HVD, LVD, or FC connectors. The particular drive interface is specified by the ordering feature code on the IBM 3584 model type:

- Feature #1454, LTO Ultrium 1 LVD Drive Canister
- Feature #1455, LTO Ultrium 1 HVD Drive Canister
- Feature #1456, LTO Ultrium 1 FC-AL Drive Canister
- Feature #1474, LTO Ultrium 2 LVD Drive Canister
- Feature #1475, LTO Ultrium 2 HVD Drive Canister
- Feature #1476, LTO Ultrium 2 Fibre Drive Canister

At least one of these drive features must be ordered on the initial L32 for a new library, and a maximum of 12 of these features may be added to each library frame model type. The features may be intermixed.

Although the IBM LTO Ultrium drive modules are the same for all IBM LTO libraries, the tape drive assembly used in the IBM 3584 libraries (Figure 8-6) is packaged uniquely. Therefore, the drives cannot be interchanged between library models. The tape drive assembly contains the drive power supply and the LTO drive (HVD, LVD or FC) itself. Each drive power supply is strong enough to support two tape drives.

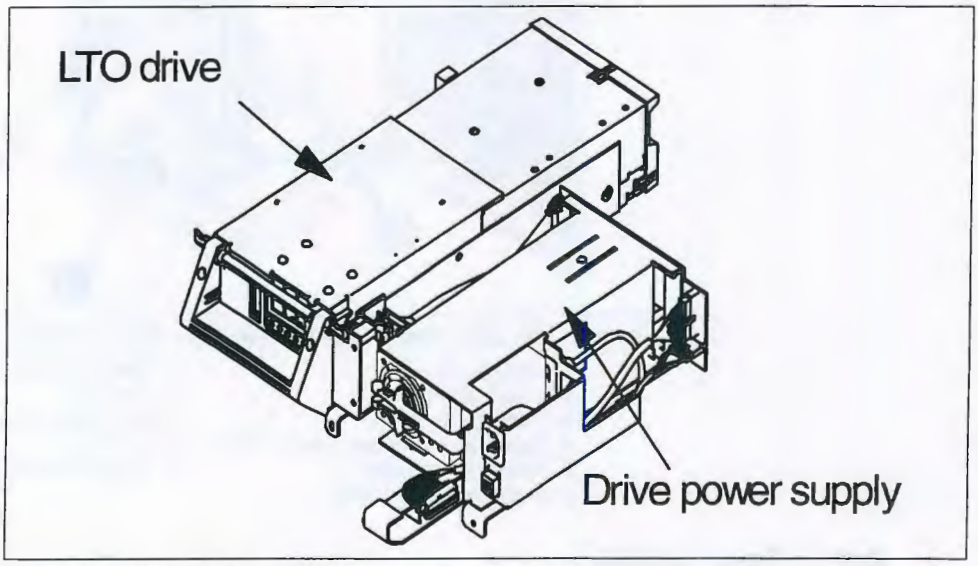


Figure 8-6 IBM 3584 LTO Ultrium tape drive assembly

For redundancy reasons, two drive power supplies deliver power for each two drives, as shown in Figure 8-7 on page 167. If one drive power supply fails, then the second power supply provides power for both drives, and both drives continue running.

10585
A.

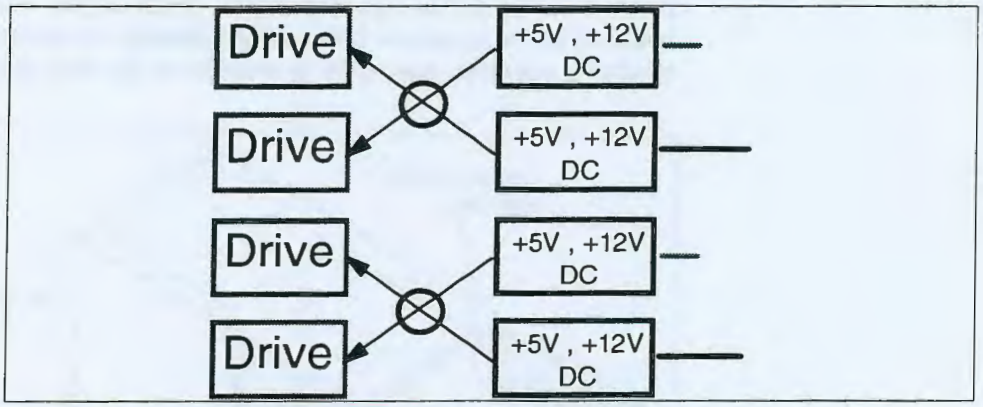


Figure 8-7 Redundant drive power supply

8.2.2 Library control systems: frame control assembly

A library control system is required for a library to operate. Conventional libraries, such as the IBM 3494, use a single library controller that handles all of the different inputs and controller output commands. The IBM 3584 uses a system of distributed embedded controllers. There are controllers, each with its own processor, for the operator panel, the accessor controller that handles the accessor and gripper, XY controller for the X and Y movements and medium changer controller for handling the commands coming from the host (Figure 8-8).

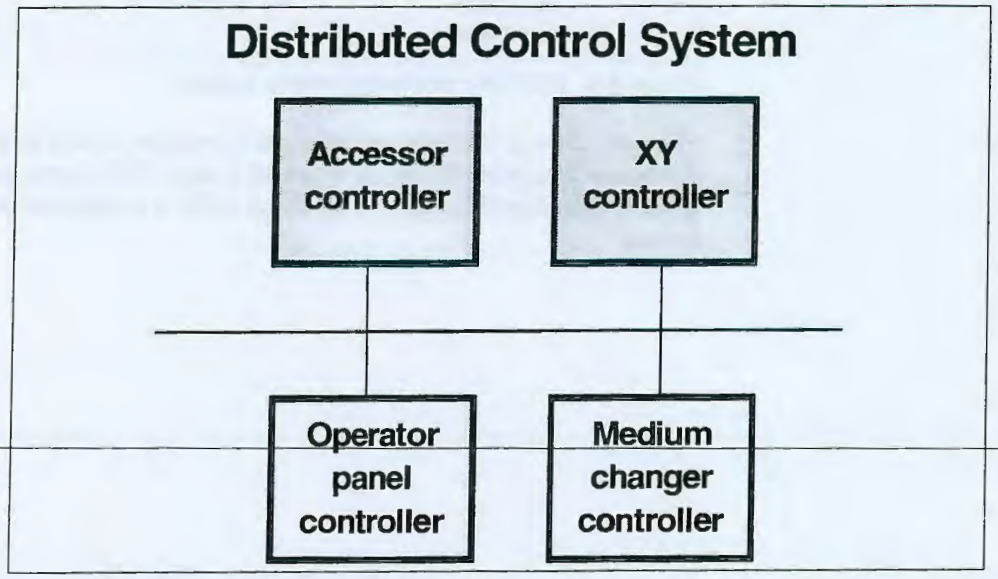


Figure 8-8 IBM 3584 distributed control system

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 1344
Doc. 3698

The four controllers are in different locations. The operator panel controller is located directly on the Operator Panel. The accessor and XY controllers are attached to the accessor. The medium changer controller, which is hosted within the frame controller assembly, is mounted in the rear of the frame (Figure 8-9).

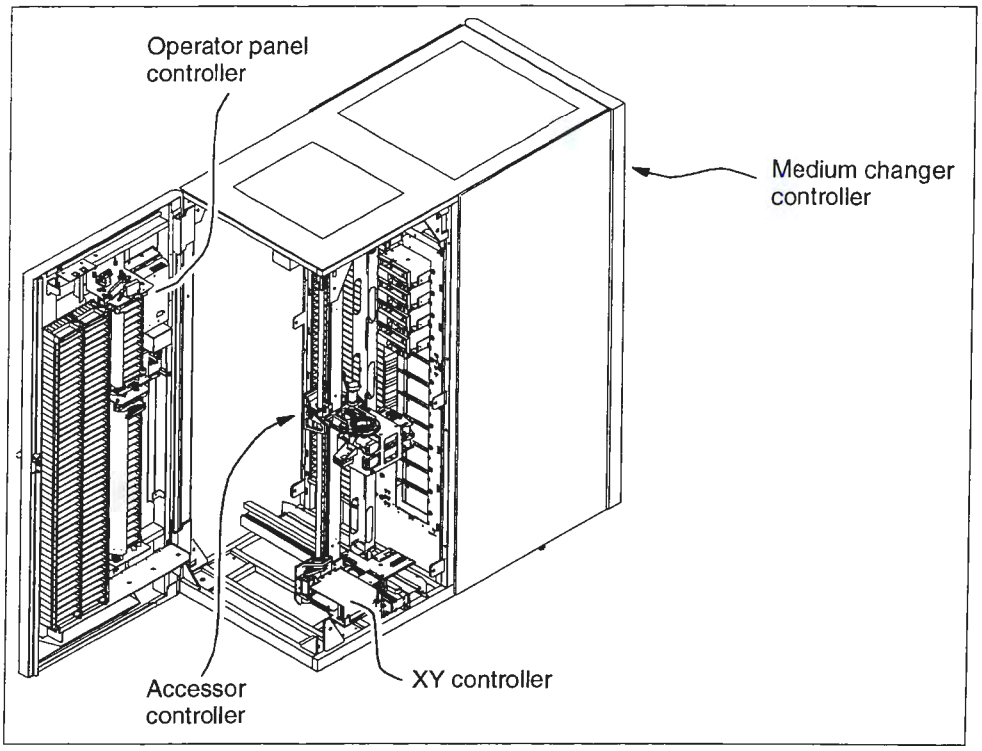


Figure 8-9 IBM 3584 distributed control system

For redundancy, the medium changer controller, which is part of the frame controller assembly (FCA), is required in each D32 frame where at least one tape drive is installed (Figure 8-10 on page 169). It is optional in a D32 with no tape drives.

10583
CA

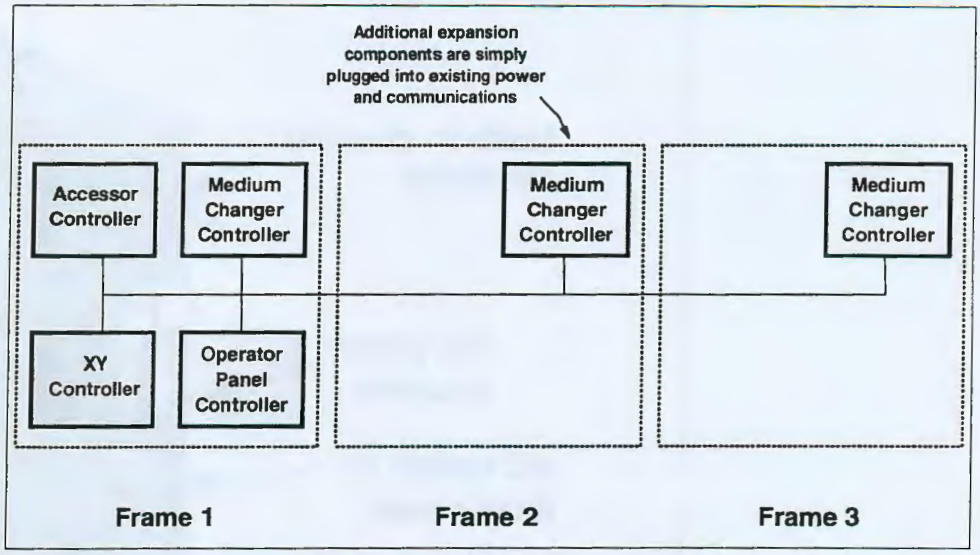


Figure 8-10 Redundant medium changer controller

The frame controller assembly (FCA) (see Figure 8-11 on page 170) is a canister containing:

- Medium changer controller
- AC outlets for tape drive power supplies
- DC power supplies for the whole library controlller
- Circuit breakers
- Incoming main AC power

The FCA for the L-Frame contains two DC power supplies; actually, only one DC power supply is needed to operate the whole IBM 3584 library. Before support was provided for 16 frames, all additional FCAs in D-Frames included one extra DC power supply for redundancy. With support for 16 frames, the additional FCAs in the D-Frames no longer have a default-installed DC power supply.

With support for 16 frames, however, you can order additional DC power supplies (FC #1902) for the D32 frames. This makes sense if not using the Dual AC power options (FC #1901); see 8.5.4, "Power and cooling specifications" on page 191. If you wish, an IBM Customer Engineer can put one of the two DC power supplies from the L-Frame into another FCA in a D-Frame to provide redundancy for both AC and DC power.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1345
3698
Doc.

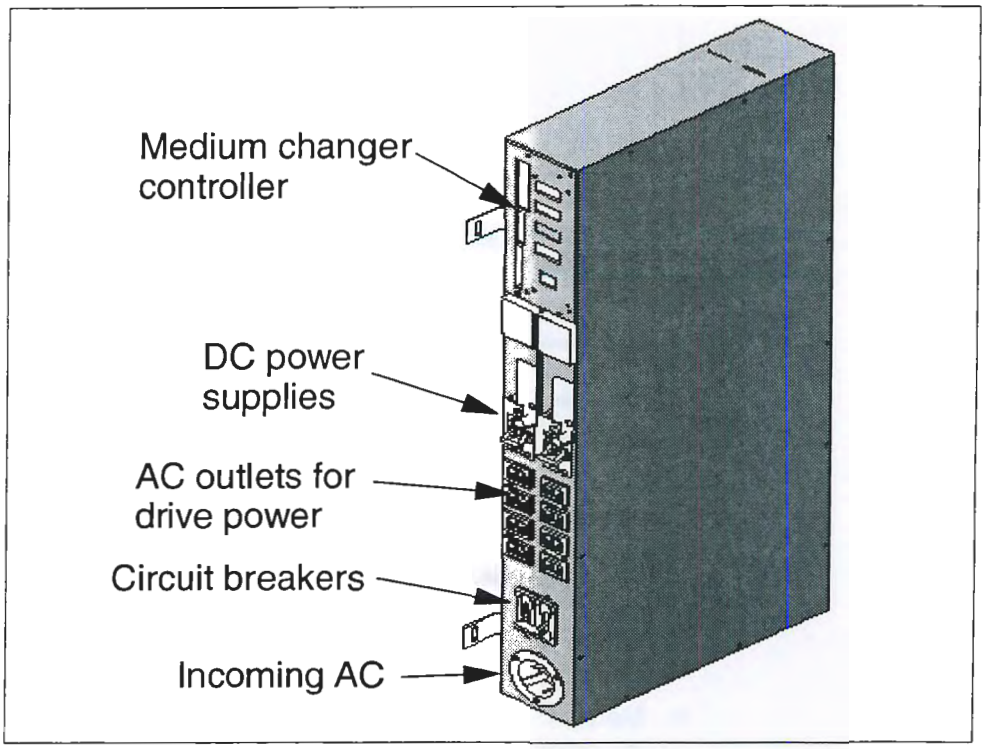


Figure 8-11 Frame controller assembly

The advantages of a distributed control system are:

- Improved reliability
  - Reduces single points of failure
  - Smaller FRU components
- Simplified library repair
  - Functionality is isolated to a single area of the library.
- Easier upgrades
  - Distributed components only require power and communication wires.
  - Modular design for "building block" approach.
- More performance than a single library controller
  - Each major library component has its own processor.

8.2.3 Operator interface

The operator interface is located on the front of the L32 frame (see Figure 8-2 on page 162) and provides a set of indicators and controls that allows an operator to perform operations and determine library status. The panel consists of the library power switch, a power-on indicator, a touch-screen LCD and controller, and the

10581
A.

controller for the I/O station. The operator panel controller is located inside the library behind the operator panel (number 11 in Figure 8-5 on page 165). It is a logic card that facilitates communication between the operator panel and the accessor controller. The operator panel controller posts status and information about the sensing and locking of the I/O station to the operator panel LCD.

The operator panel touch screen (Figure 8-12) consists of the touch keys area and the activity and status screen. The activity screen displays *LmultCD* on the touch screen when the library is ready (that is, when host applications may interact with the library). The first line on the screen shows the current level of library firmware and the panel screen number. The left field on the second line indicates that the library is either ready, not ready (not interacting with host applications), or initializing. The right field indicates the status of one or more I/O stations. The activity screen also shows the current activity in a large font, and provides a history of preceding operations in a smaller font. Operations are listed from top to bottom with the most recent at the top. The activity screen automatically displays an error message when an error condition is detected. See 8.9, "Operator displays and buttons" on page 196 for more information.

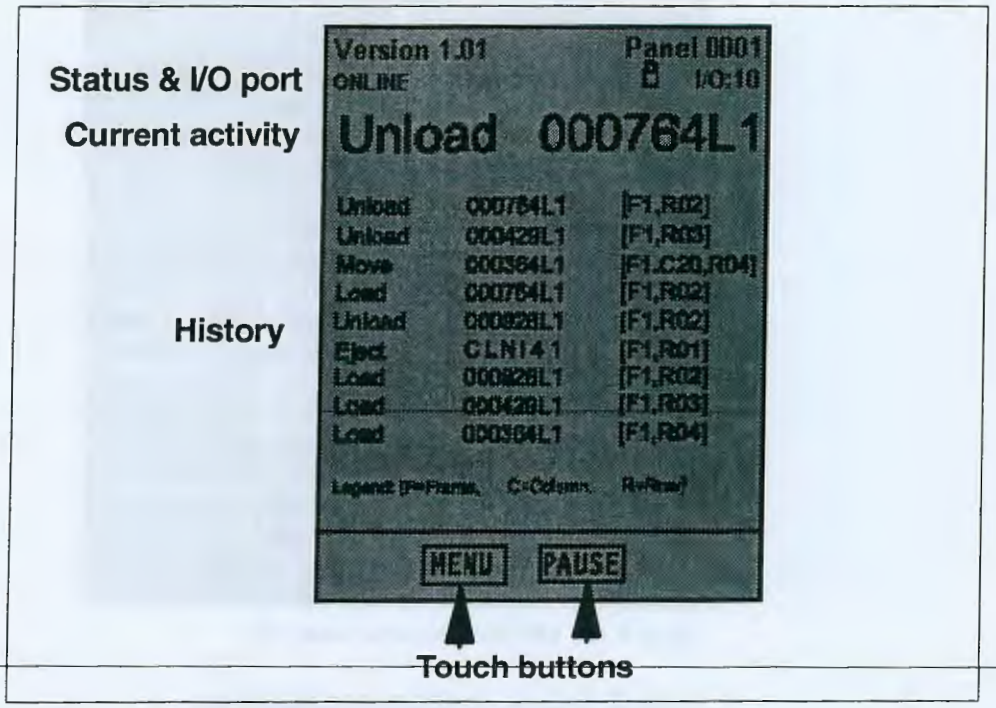


Figure 8-12 Operator panel

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1346
Doc 3698

8.2.4 Robotic cartridge accessor

The cartridge accessor is the assembly that moves tape cartridges between storage slots, tape drives, and the I/O station (number 3 in Figure 8-5 on page 165). The accessor assembly moves horizontally through the library frames using a rail system (number 2 in Figure 8-5 on page 165); it uses both top and bottom rails.

The accessor assembly consists of a dual gripper (number 4 in Figure 8-5 on page 165 and in more detail in Figure 8-13) mounted on a vertical pole. The gripper can move up and down vertically, and also rotates to access cartridge slots on both the back walls and front doors of the library frames. A barcode reader is mounted on the accessor and can scan the cartridges in one frame in less than a minute.

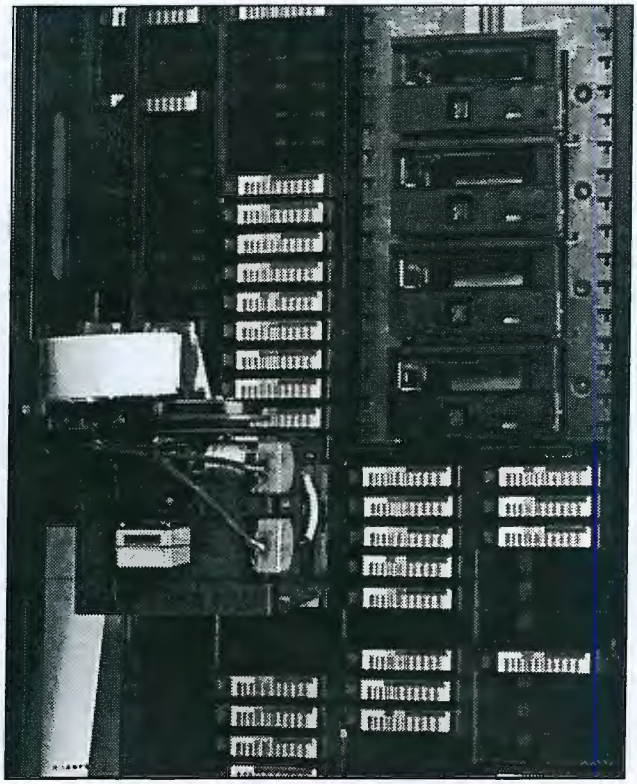


Figure 8-13 IBM 3584 accessor assembly

X- and Y-axis motion assemblies

These assemblies include a controller (circuit board) for the Controller Area Network interface, servo motor, pinion drive gear, and lead screw. These assemblies provide the motive force to move the accessor side to side (on the

X-axis) and up and down (on the Y-axis). The controller part of this assembly is referred to as the XY controller.

Pivot assembly

This group of parts provides a mounting platform for the gripper mechanism and the barcode reader. This assembly is capable of 180-degree rotation around the vertical axis.

Cartridge gripper

This electromechanical device (mounted on the pivot assembly) gets or puts cartridges from or to a storage slot, tape drive, or I/O station. The gripper is independently controlled and can grip a single cartridge. There are two grippers on the pivot assembly (Gripper 1 and Gripper 2).

Many libraries offer support for different drives and media, such as LTO, DLT, or AIT. Typically, they use a universal gripper for cartridge handling; clam shell grippers are a common design approach. The main problem with this approach is performance and reliability. A "catch-all" gripper cannot be optimized for each different media type. The LTO cartridge was designed with automation in mind, and IBM was a key player in this effort. The cartridge contains automation handling features, such as the notches seen in Figure 8-14. The IBM 3584 gripper takes advantage of the handling features and uses hooks tor handling the cartridge. This approach offers significant performance improvements as described in 8.3, "Performance" on page 186, and is more reliable than a catch-all gripper.

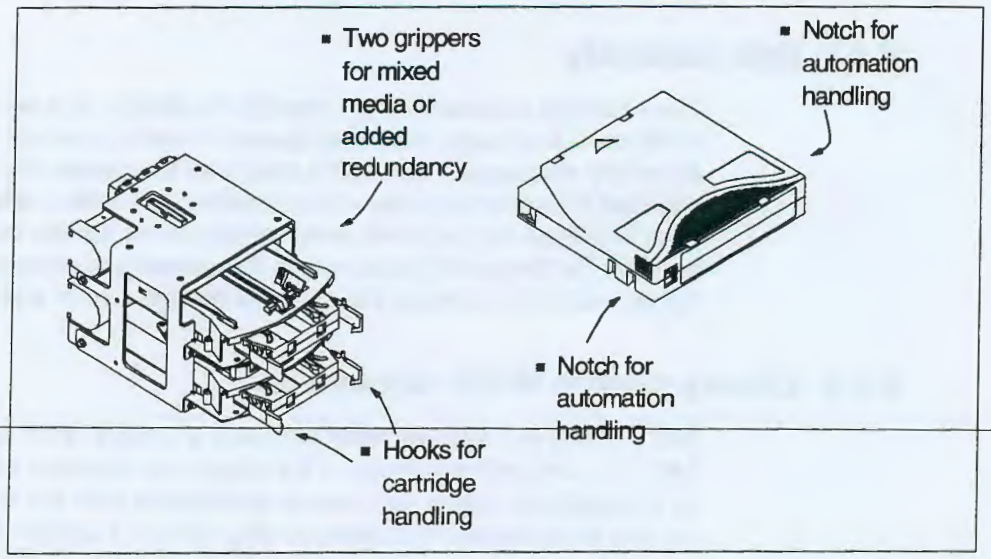


Figure 8-14 IBM 3584 Gripper

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1347
Doc 3698

The use of a dual-gripper accessor reduces the time taken to move cartridges in the library and can improve overall performance on large libraries. It increases redundancy and reliability. Note that library functions are controlled by host application software, and to make use of the dual gripper function, the software itself must be able to use two grippers simultaneously. If it does not, then the library will function as if it had only a single gripper. If only one gripper is used at a time, the library periodically switches between both grippers to balance use.

Barcode reader

The barcode reader reads the barcode on a label that is attached to a cartridge or at the rear of every storage slot (which indicates an empty storage slot). The barcode reader is mounted on the pivot assembly, and is used during inventories, audits, insertions, and inventory updates. The inventory is updated whenever the door is opened, and determines whether cartridges have been added to, removed from, or moved within the library).

Because all storage slots have empty storage cell labels, the library can easily and quickly recognize if there is a labelled cartridge or an empty storage slot in every location. This eliminates the need to reread or manually intervene in storage cells if no label is readable. Without this approach the library cannot differentiate between a slot that is unlabeled, badly labelled, or empty.

Calibration sensor

This provides a means to locate certain positions within the library very precisely during the calibration operation. The calibration sensor is mounted on the underside of Gripper 1. All positions are calculated from these locating positions.

8.2.5 Rail assembly

The cartridge accessor moves through the library on a rail assembly (number 2 in Figure 8-5 on page 165). The system consists primarily of a main rail assembly and support rail, and a trough for the power and control cable. The main rail assembly includes a main bearing way with a rack gear. Its support rail is an L-shaped rail that runs along the top of the frames and provides smooth transport for the cartridge accessor. The power and control cable is kept clear of the accessor in a covered trough at the bottom rear of the library.

8.2.6 Library centric WWN convention

Every device in a SAN environment uses a unique WWN for identification in the SAN. In a conventional library, if the drives are swapped then the WWN will also be changed and hence you have to reconfigure both the SAN and the server. If you are using persistent binding on your server, a server reboot is also necessary.

10577
A.

The IBM 3584 assigns the WWNs to the drives. This technique is referred to as "library centric world wide names." Every potential drive slot is assigned with a unique WWN. If a drive is replaced, then the new drives gets the same WWN as the old one. This is controlled by the FCA. Because of this library behavior, you can easily identify the position of the drive in the library by the WWN. The last two digits represent the drive's location in the library. The last digit indicates the drive row, starting from 1, and the second last indicates the frame, counting from 0. The remaining digits are encoded with the vendor ID and the library serial number, ensuring that every drive has a unique WWN. Figure 8-15 shows the drive WWNs in an IBM 3584.

```
World Wide Node Names                          Panel 0126

Key: [F=Frame, R=Row]

[F1,R01]  5005 0763 0041 0001
[F1,R02]  5005 0763 0041 0002
[F1,R03]  5005 0763 0041 0003
[F1,R04]  5005 0763 0041 0004
[F1,R05]  5005 0763 0041 0005
[F1,R06]  5005 0763 0041 0006
[F1,R07]  5005 0763 0041 0007
[F1,R08]  5005 0763 0041 0008

[BACK]      [  UP  ]      [DOWN]
```

Figure 8-15 Drive WWNs of an IBM 3584

8.2.7 Control path failover

Alternate path support, currently available only for AIX hosts, configures multiple physical control paths to the same logical library within the device driver and provides automatic failover to an alternate control path when a permanent error occurs on one path. This is transparent to the running application.

For example, consider a simple multi-path architecture connection consisting of two HBAs in an AIX host that are connected to a library with two or more drives (Figure 8-16 on page 176). Two drives have the control ports enabled. The two HBAs are connected to the first and second control port drives, respectively. This simple configuration provides two physical control paths to the library for

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls Nº 1348
Doc. 3698

redundancy if one path from an HBA to the library fails. When the AIX server is booted or **cfgmgr** is run, each HBA detects a control port to the library and two medium changer devices, smc0 and smc1, will be configured. Each logical device is a physical path to the same library; however, an application can open and use only one logical device at a time, either smc0 or smc1.

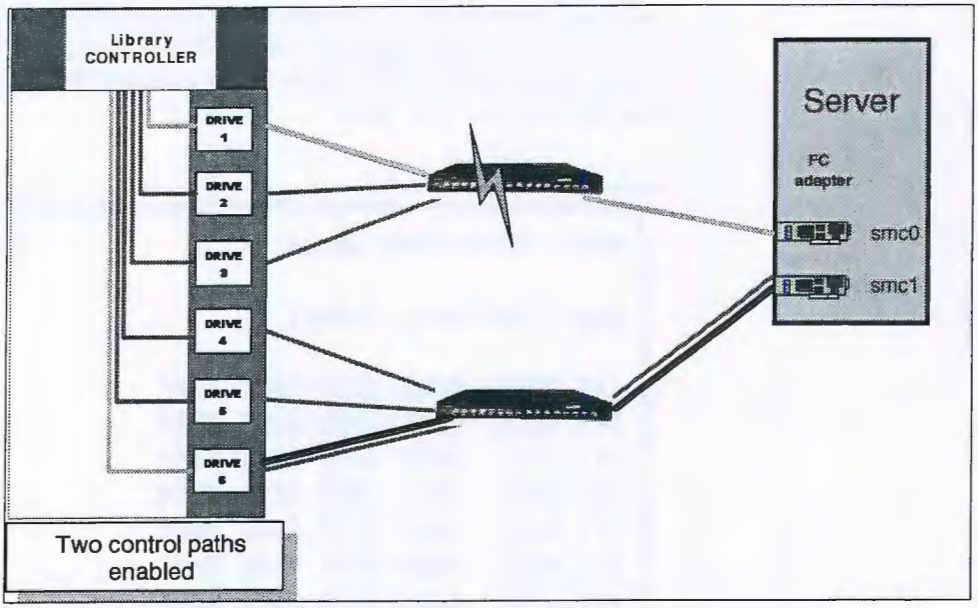


Figure 8-16 Redundant control paths to the library controller

Without the Atape (device driver) alternate pathing support, if an application opens smc0 and a permanent path error occurs (because of an HBA, cable, or drive control port failure), the current command to the library fails. It is possible to initiate manual failover by changing the device path to the alternate path (smc1), but this is a manual operation and the last failing command has to be re-sent.

When the alternate pathing support is enabled on both smc0 and smc1, the device driver configures them internally as a single device with multiple paths. The application can still open and use only one logical device at a time (either smc0 or smc1). If an application opens smc0 and a permanent path error occurs, the current operation continues on the alternate path without interrupting the application.

8.2.8 StorWatch

The library's Web interface, known as the IBM TotalStorage UltraScalable Tape Library Specialist, enables operators and administrators to manage storage devices from any location in an enterprise. The IBM 3584 StorWatch Specialist

10575
A.

allows direct communication with an IBM 3584 and provides a full range of end user, operator, and administrator tasks, which can be executed remotely.

The StorWatch Specialist requires a Category 5 Ethernet cable (not supplied with the tape library).

Multiple simultaneous Web clients

Each Ethernet capable medium changer controller (MCC) on the IBM 3584 allows five simultaneous StorWatch users.

Individual Web login IDs and passwords

For the IBM 3584, the Web user interface supports a list of users that can access various areas of the Web user interface. Each user has a 30-character name, a 15-character login ID, a 15-character password, and an access level. The access level defines the level of Web access that the user is allowed. The two levels of access are "user" for non-destructive Web access and "super user" for more advanced functionality such as moving cartridges and configuring the library. User and super user login IDs cannot create, modify, or change any login IDs. Any login ID can change their own password. The special login ID "admin" can create, modify, and destroy all login IDs except the admin ID.

Multiple simultaneous Web clients and individual Web ID functions can be made available to existing IBM 3584 libraries by upgrading to the latest firmware.

8.2.9 I/O station

Each L32 frame has a standard 10-slot cartridge input/output station for importing or exporting cartridges from the library without requiring a re-inventory or interruption of library operations. An optional feature (FC # 1657) provides 20 additional input/output slots.

8.2.10 Reliability

The IBM 3584 is designed for high availability and reliability. Most essential components are redundant, so there is no single point of failure. Most of these components have been described previously. Here is a summary of the high-availability features and components of the IBM 3584:

- Redundant grippers
  - A failure of one gripper will cause the library to switch to a second gripper.
- Redundant library power
  - Each drive frame provides one additional power supply.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1349
Doc 3698

- A single frame library contains one redundant power supply.
  - Optional redundant frame power available
- The library can operate on a single power supply.
- The library automatically monitors and controls redundant power distribution.

- Redundant drive power
  - Each drive bay power module supplies redundant power to another drive bay.
- Redundant control paths
  - Any LTO drive can be used as a library control path.
  - Automatic control path failover available for AIX.
- Redundant copies of Vital Library Data
  - Includes configuration data, calibration data, setup data, etc.
  - One processor card contains the primary copy and another processor card contains a backup copy.
  - Backup/restore process is completely automated
- Redundant copies of library firmware
  - Each processor card contains the firmware for every other processor card.
  - Component replacement is simplified.
  - Each processor card contains two copies of operational firmware.
  - Protects the library from potentially harmful firmware update disruptions.
  - Helps reduce the risk of memory failures.
- Closed loop servo systems
  - Includes horizontal motion, vertical motion, pivot motion, gripper extend, and retract motion.
  - Each servo system uses feedback.
  - Velocity and position are monitored.
  - Allows higher performance (as shown in Table 8-5 on page 187).
    - Knowing velocity and position allows greater control.
  - Closed loop is more reliable.
  - Collisions and gripper damage can be avoided by monitoring position and velocity.

1057
A

8.2.11 Service

This section describes support and service for the IBM 3584.

Call-home

The library calls an IBM Support Center when an error occurs. The library reports codes indicating the replacement parts that may be required and the urgency of the problem. No-charge feature #2710 (Remote Support Facility) provides a modem and cable (15.2 m or 50 feet). The customer must provide an analog phone line to use the call-home feature. This phone line should be close to the library (within 15.2 m; 50 feet).

If a second 3584 (L32) library is installed close (within 15.2 m or 50 feet) to the first one, you can order feature #2711 (Remote Support Switch) for the second library. This feature provides a modem switch in order to share the modem from the first library. The benefit is that a single phone line can service both libraries.

For the third and every subsequent 3584, installed close to the first one (within 15.2 m or 50 feet), you can order feature #2712 (Remote Support Attachment). This provides cabling for connecting to the Remote Support Switch. A maximum of 14 libraries can be connected to the switch.

If the additional libraries are not close together, then feature #2710 and a phone line is required for each one.

Firmware

As described in 8.2.2, "Library control systems: frame control assembly" on page 167, the IBM 3584 has four control assemblies. Each of them has the complete firmware image stored on flash ROMs. The same firmware image is stored on each card, avoiding the need to keep multiple code images in sync. A node card may only use a small portion of the firmware image, but it has the whole image in its flash. The node card firmware provides the ability to communicate with other node cards. The node cards can determine the level of firmware on other node cards and can request a copy of the firmware from another node card. This ability enables the cards to operate automatically at a consistent firmware level throughout the library subsystem.

When a node card completes its Power-On Self Test (POST), it asks all of the other node cards to report their firmware levels. If it determines that another node card has a higher version of firmware, it will obtain the firmware from that node card and update its flash ROM before coming online. This ensures that when a node card FRU containing down-level firmware is installed in the library, it will be updated automatically.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1350
Doc. 3698

Each node card contains two complete copies of the firmware in flash ROM for redundancy. If a problem such as a power failure interrupts a firmware update, the node card can automatically switch to the backup copy. Another attempt can then be made to update the firmware. The update process always overwrites the damaged or oldest firmware image first, so the node cards should always have a usable level of firmware.

During replacement of tape drives, the library automatically detects the firmware version of the newly installed drive and, if needed, updates the drive firmware.

This behavior of the IBM 3584 avoids any potential for replacement parts containing a wrong firmware version.

SNMP

Occasionally, the IBM 3584 may encounter a situation that should be reported, such as an open door that causes the library to stop. Because many servers can attach to the IBM 3584 by differing attachment methods, the library provides a standard TCP/IP protocol called Simple Network Management Protocol (SNMP) to send alerts about conditions (such as an opened door) over a TCP/IP LAN network to an SNMP monitoring server. These alerts are called SNMP traps. Using the information supplied in each SNMP trap, the monitoring server (together with customer-supplied software) can alert operations staff of possible problems or operator interventions that occur. Many monitoring servers (such as Tivoli NetView®) can be used to send e-mail or pager notifications when they receive an SNMP alert.

The monitoring server must be loaded with systems management software that can receive and process the trap, or the trap will be discarded. SNMP trap support does not provide a mechanism for the operator to gather more information about a problem or to query the library about its current status.

If your systems management software includes an SNMP compiler, you may not need to manually interpret SNMP traps but you will need the library's Management Information Base (MIB). The MIB contains units of information that specifically describe an aspect of a system, such as the system name, hardware number, or communications configuration. Obtain the MIB for the IBM 3584 from:

`ftp://ftp.software.ibm.com/storage/358x/3584`

Configuration

The IBM 3584 automatically configures and calibrates itself as initiated from the operator panel or StorWatch. New hardware is automatically discovered. This eliminates the user or IBM engineer from entering invalid data.

10571
A-

8.2.12 Capacity

The overall size of an IBM 3584 library frame (either L32 or D32), allows for up to 10 storage columns: five columns located on the back wall of the frame and five on the interior of the door (see Figure 8-17 on page 182 and Figure 8-18 on page 184). Each column is made up of 44 slots, so the maximum available cartridge storage capacity of the D32 frame is 440 (44 times 10).

In practice, some installed library components take up space inside the library frames, which reduces the space available for cartridge slots. Some of these library components are installed as standard (for example, in the model L32 where the maximum capacity is 281), and some are variable, for example the installation of drives in either frame model type).

This section explains the layout of the cartridge slots in the interior of each of the model types and provides tables to calculate the library capacity for various configurations.

Model L32

In the Model L32, the robotic home position utilizes the area to the left of the frame and prevents access to any cartridge slots in that area. This means that there are eight cartridge slot columns in the model L32, four on the back wall of the frame and four on the inside of the door. In addition, the I/O station takes up space on the inside of the door, and the drive positions take up space on the back wall, further reducing the cartridge slots available.

The layout of the cartridge slots and columns is shown in Figure 8-17 on page 182. The columns are numbered with those on the back wall designated as numbers 1, 3, 5, and 7, while those inside the door are numbers 2, 4, 6, and 8. Therefore column number 1 faces column number 2, 3 faces 4, and so on.

In order to provide a less expensive entry level tape solution, only columns 1, 3, 5, and 7 (those on the back wall) are accessible in the standard L32 frame. If greater capacity is needed, order a chargeable feature (the capacity expansion feature, feature codes #1603 or #1653) to make columns 2, 4, 6, and 8 available to store cartridges (noting that some of the slot positions in columns 2 and 4 are occupied by the cartridge I/O station, as shown in Figure 8-17 on page 182). The capacity expansion feature must be added before expanding the library with any D32 expansion frames.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1351
Doc 3698

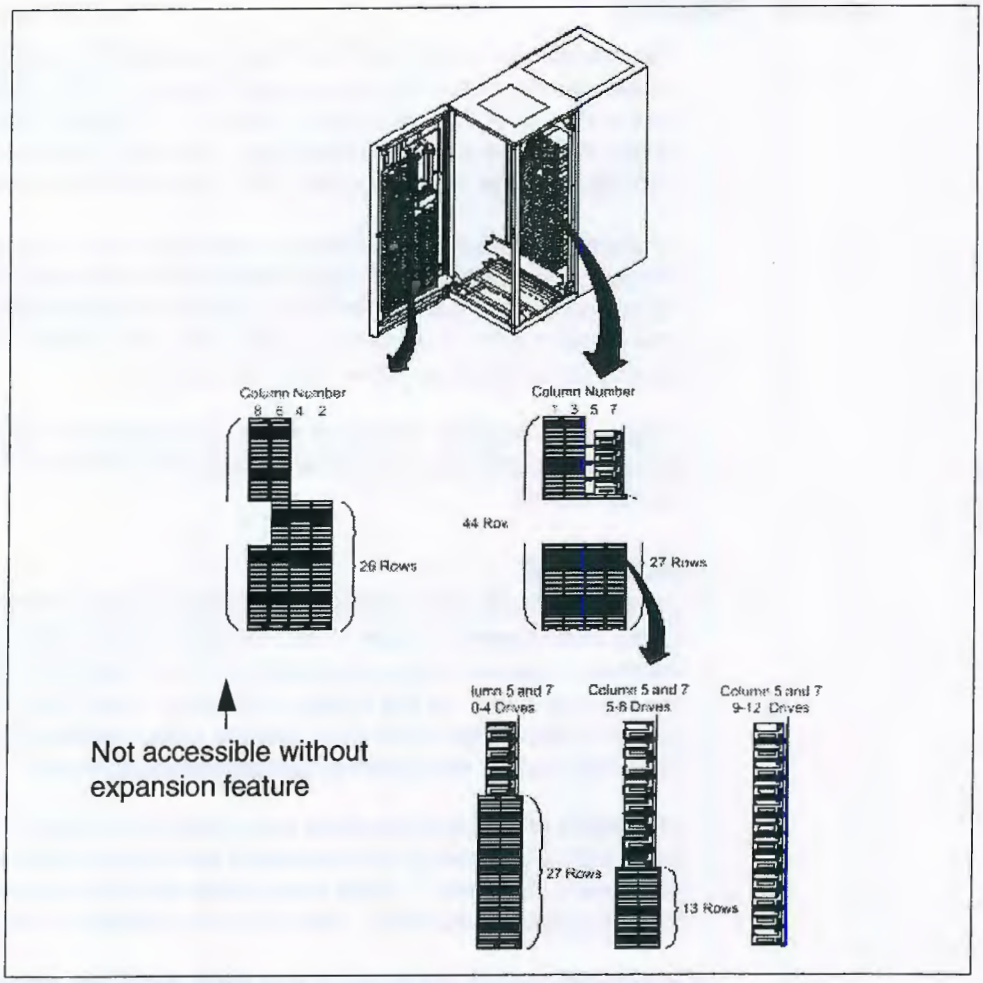


Figure 8-17 IBM 3584-L32 base frame showing cartridge slot components

The tape drives inside the L32 frame take up space in columns 5 and 7 on the right side of the back wall of the library as shown in Figure 8-17. As the drives are added, there is an incremental reduction in cartridge storage space. At least one drive must be installed in the L32 frame, and since drive positions are reserved in sets of four, this removes one-third of the cartridge slots from columns 5 and 7. When you install the fifth drive, this removes another third of the slots from columns 5 and 7, until finally, when the ninth drive is installed, the drive positions take up all of the space where columns 5 and 7 would have been located.

The very first slot in the L32 frame (column1 row 1) at the top left side of the back wall is always reserved for a diagnostic cartridge.

The next two tables summarize the available slots in the Model L32, both *without* the capacity expansion feature (Table 8-1) and *with* it (Table 8-2).

Table 8-1 IBM 3584-L32 slot capacity without capacity expansion feature

Column #	1 to 4 drives	5 to 8 drives	9 to 12 drives
1 (back wall)	43	43	43
3 (back wall)	44	44	44
5 (back wall)	27	13	0
7 (back wall)	27	13	0
2,4,6,8 (door)	Not accessible	Not accessible	Not accessible
Total	141	113	87

Table 8-2 IBM 3584-L32 slot capacity with capacity expansion feature

Column #	1 to 4 drives	5 to 8 drives	9 to 12 drives
1 (back wall)	43	43	43
3 (back wall)	44	44	44
5 (back wall)	27	13	0
7 (back wall)	27	13	0
2 (door)	26	26	26
4 (door)	26	26	26
6 (door)	44	44	44
8 (door)	44	44	44
Total	281	253	227

Model D32

In the Model D32, all 10 columns are available for use with cartridge slots. A D32 may be added to the library without any installed drives, so 10 columns of 44 slots each are available giving a total storage capability of 440 cartridges.

The columns are arranged and numbered similarly to the L32, but with two additional columns available. The layout of the cartridge slots and columns is shown in Figure 8-18 on page 184. The columns are numbered: the back wall columns are numbers 1, 3, 5, 7, and 9, while those inside the door are numbers 2, 4, 6, 8, and 10. As in the L32, column number 1 faces column number 2, 3 faces 4, and so on.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1352
3698
Doc.

All 10 columns are accessible as soon as the D32 is installed; there is no need for any capacity-expansion feature for this frame. However, note that the L32 must be fully configured for capacity before adding any model D32 frames to it. In other words, the L32 must have the capacity expansion feature installed.

The robotic home position is in the L32 and there is only one I/O station per library, which is also located in the door of the L32, so the installation of tape drives is the only factor reducing the available cartridge storage slots in the D32.

The capacity expansion feature may be ordered either for installation at the manufacturing plant as feature #1653 or as a field upgrade, feature #1603.

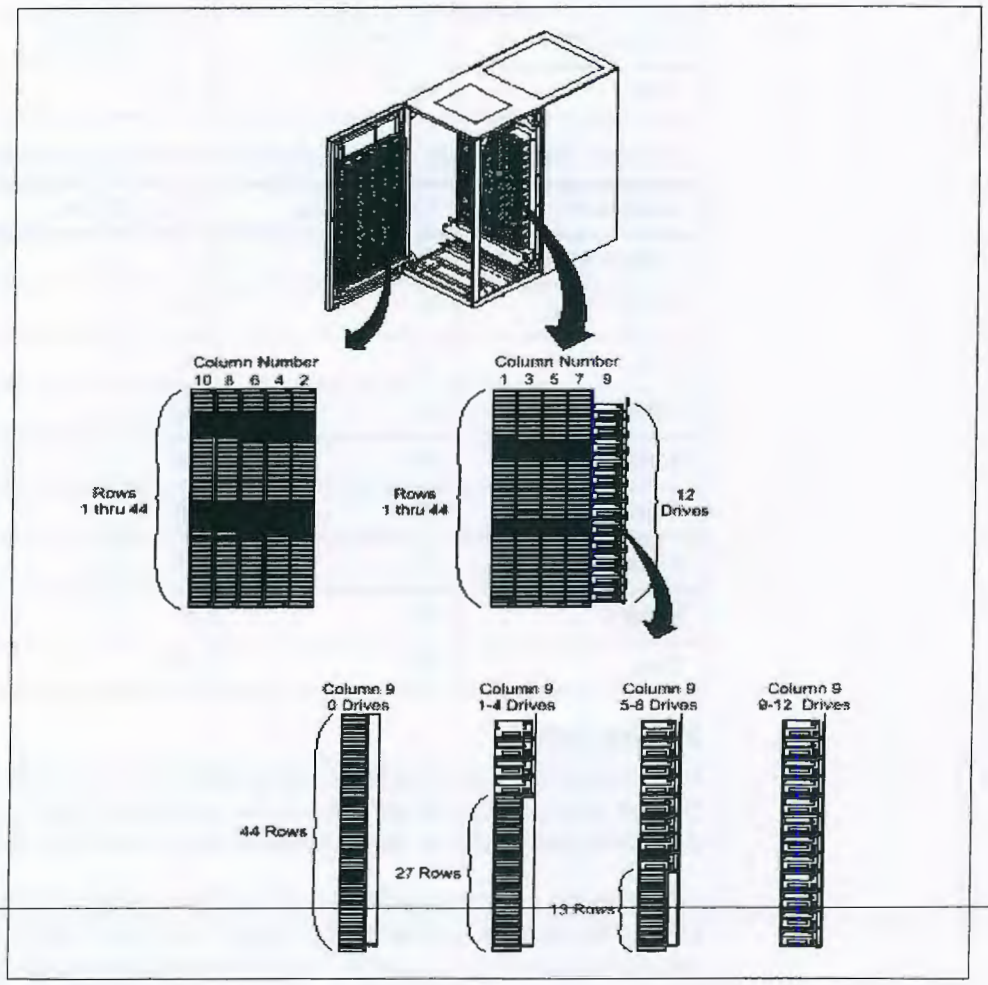


Figure 8-18 IBM 3584-D32 expansion frame showing slot components

10567
A

The tape drives in the D32 are located (as in the L32) on the right side of the back wall of the library, as shown in Figure 8-18 on page 184. However, the standard layout of hardware components in the L32 differs from the D32, so space utilization is also slightly different. The tape drives in the D32 use space only in column 9 so that even with the maximum 12 drives installed, only the 44 slots in column 9 are unavailable.

As drives are installed in the D32, there is an incremental reduction in cartridge storage space in column 9. Again the drive positions are reserved in sets of four, so that installing the first drive in the frame removes one-third of the cartridge slots from columns 9. Installing the fifth drive in the frame removes another third of the slots in column 9, until finally when the ninth drive is installed, the drive positions take up all of the space where column 9 would have been located. Table 8-3 summarizes the available slots in the D32 frame.

Table 8-3 IBM 3584-D32 cartridge slot capacity

Column #	0 drives	1 to 4 drives	5 to 8 drives	9 to 12 drives
1 (back wall)	44	44	44	44
3 (back wall)	44	44	44	44
5 (back wall)	44	44	44	44
7 (back wall)	44	44	44	44
9 (back wall)	44	27	13	0
2 (door)	44	44	44	44
4 (door)	44	44	44	44
6 (door)	44	44	44	44
8 (door)	44	44	44	44
10 (door)	44	44	44	44
Total	440	423	409	396

8.2.13 Adding and removing cartridges

A 10-cartridge I/O station[1] on the front door of the IBM 3584 Model L32 enables insertion and removal of cartridges from the library enclosure without interrupting library operation. Figure 8-2 on page 162 shows the position of the I/O station from outside the library, and the internal side of the frame door is shown as number 10 of Figure 8-5 on page 165.

[1] An optional additional 20-cartridge I/O station is available.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1353
Doc. 3698

The I/O station is controlled by the host application software that uses the library or from the operator panel. Insertion of cartridges into the I/O station alerts the application software, which registers the additional cartridges and their status in its database and then instructs the accessor to move the new cartridges into library slots. The slot location of each cartridge is held in the host application software database.

For bulk-loading of cartridges (more than 10), you can open any library frame door and insert cartridges in any available slots in the frame. When the door is closed, the library will perform a cartridge inventory operation, which checks to determine whether each cartridge storage slot in the frame is empty or full and scans the cartridge barcode labels. When the library performs an automatic inventory in this way, the inventory will occur only for those frames whose doors had been opened.

A cartridge inventory operation occurs whenever you:

- Power on the library
- Issue the SCSI command Initialize Element Status with Range[2]
- Select Inventory from the Manual Operations menu
- Select the appropriate menus from the UltraScalable Specialist Web interface
- Close the front door after manually accessing the library

When the library performs an automatic inventory because the front door was closed, the inventory occurs only for those frames whose doors have been opened. A door lock is provided to restrict physical access to cartridges in the library. This can be used to secure the cartridges and prevent unauthorized library access. Although the time required for the library to inventory cartridges is less than 60 seconds per frame, the door lock reduces the possibility of frames being opened in error and causing unnecessary inventory activity.

There is also a safety switch in the frame door (number 9 in Figure 8-5 on page 165) that shuts down the power to the cartridge accessor whenever the front door is opened.

8.3 Performance

The performance capability of a tape library solution depends on both the individual bandwidth capability of the drives and data bus and the speed of the robotic handling. The degree of importance for each of these elements depends on the quantity of data transferred during one operation. For example, when reading or writing large files (larger than 800 MB) to tape, then the data rate of

[2] The 3584 library tracks the logical location of all elements in the library by performing an automatic inventory as required (thus, the SCSI Initialize Element Status command is allowed but ignored).

10505
A.

the tape drive will be the overriding contributor to the speed of the operation. However, for reading or writing many small files (25 MB or less) to different tapes then the cartridge move and load times become the overriding contributor.

The following elements contribute to the high-performance capabilities of IBM 3584 libraries:

- Library bandwidth
  You see the bandwidth of the IBM 3584 in Table 8-4 relating to the drive performance given in 2.4.4, "Performance" on page 35. Values in the compressed column assume a compression of 2:1.

Table 8-4 IBM 3584 bandwidth

Tape drives	LTO Ultrium 1 native	LTO Ultrium 1 compressed	LTO Ultrium 2 native	LTO Ultrium 2 compressed
72	3.8 TB/h	7.7 TB/h	9.0 TB/h	18.1 TB/h
192	10.3 TB/h	20.7 TB/h	24.1 TB/h	47.4 TB/h

- Cartridge move time
  In a single-frame IBM 3584, the typical time to move a cartridge from a cartridge storage slot to a tape drive, for example, is less than 2.5 seconds, For a six-frame configuration it only increases to 4.5 seconds, and for the maximum 16 frames, the average move time is still only 9 seconds, as shown in Table 8-5.

Table 8-5 Library performance

Library configuration	Average move times	Mounts per hour
1 Frame	2.4 seconds	600
2 Frames	2.5 seconds	515
4 Frames	3.0 seconds	405
6 Frames	3.8 seconds	340
8 Frames	4.9 seconds	265
12 Frames	6.5 seconds	205
16 Frames	8.0 seconds	165

Here are some thoughts about the relationship between drives per library and mounts per hour:

- If you do mainly full backups that fill entire cartridges at a time, an Ultrium 1 drive needs about 111 minutes and an Ultrium 2 about 95 minutes to fill a cartridge. This means that you have to mount an Ultrium 1

RQS nº 03/2005 - CN
CPMI CORREIOS
Nº 1354
Doc 3698

drive 0.54 times per hour and an Ultrium 2 drive 0.63 times per hour. Even in a 16-frame library with 192 drives, you should not encounter any performance problems stemming from the mount capability of the library.

- If you mount a cartridge, read or write a small piece of data, unmount the cartridge, and repeat, then a drive is busy for approximately three minutes to execute this cycle (load, search, read/write, rewind, unload). This means you might mount a cartridge not more than 20 times per hour. In this worst-case scenario, you may see mount performance affecting library performance.

Both of these theoretical cases should help you determine how many tape drives you should install in the library to avoid mount performance problems.

- Library inventory time
  During normal use of the IBM 3584, for bulk loading of cartridges the library will perform an inventory operation to check the (possibly new) content of the cartridge storage slots. During this time, the accessor is occupied scanning the bar code labels and empty slots.

  The inventory process for the IBM 3584 is performed very efficiently, usually taking less than 60 seconds per frame.

8.4 Upgrades and optional features

The IBM 3584 has a number of optional additional features. These enhance the library by providing extra functions, additional capacity, higher reliability, and greater serviceability.

8.4.1 Upgrade features

You can install an entry-level system with moderate capacity then upgrade it as capacity requirements increase by ordering extra features. A single-frame, single-drive system can be expanded over time to become a fully configured 16-frame 192-drive library.

Adding cartridge capacity

You can add capacity to an installed library in several ways:

- The #1603 capacity expansion feature can be applied to a standard model L32 (one without #1603 or #1653 already installed). This feature enables the use of 140 cartridge storage cells on the inside of the door.
- Model D32 expansion frame can be added to the base L32 frame to provide a maximum of 440 extra storage slots. To provide the full capacity you must add #9001 to indicate that the frame is to be supplied without drives[3]. Up to 15

10563
A.

D32 frames can be added to the base frame for up to 6,600 additional storage slots in increments of 440.

Adding drives to the library

The minimum requirement for an IBM 3584 (either single or multiple frame) is that it contain at least one tape drive in the L32 base frame.

To add a drive to the library, you can order any of these features, which can be intermixed within the library:

- Feature #1454, LTO Ultrium 1 LVD Drive Canister
- Feature #1455, LTO Ultrium 1 HVD Drive Canister
- Feature #1456, LTO Ultrium 1 FC-AL Drive Canister
- Feature #1474, LTO Ultrium 2 LVD Drive Canister
- Feature #1475, LTO Ultrium 2 HVD Drive Canister
- Feature #1476, LTO Ultrium 2 Fibre Drive Canister

The maximum number of drives per frame (L32 or D32) is 12, creating a total of 192 drives in a 16-frame library. Be aware that as you add drives to a frame, you incrementally lose cartridge storage slots (see 8.2.12, "Capacity" on page 181).

8.4.2 Optional features

For more information about available features, see the sales manual for the IBM 3584. You can access the sales manual at:

`http://www.ibmlink.ibm.com/ussman`

8.5 Environmental specifications

The IBM 3584 is designed to be a stand-alone tape subsystem consisting of one or more frames and capable of modular expansion to provide large capacities. The frames join end to end, with the base frame on the left (viewed from the front) and the expansion frames extending to the right.

8.5.1 Physical dimensions

The IBM 3584 frames have the same physical dimensions but their weights vary according to the number of installed drives, robotics, and tape cartridges:

- Width: 72.5 cm (28.5 in)
- Depth: 152 cm (59.8 in)
- Height: 180 cm (70.9 in)

[3] Adding drives to the frames incrementally reduces the capacity

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1355
3698
Doc

Each frame has a set of casters and four leveling jackscrews. The nominal height from the bottom of the jackscrews to the top of the frame is 1840 mm (72.4 in), and can be varied by ±40 mm (±1.6 in). The shipping height of the IBM 3584 (on its casters and with jackscrews raised) is 1800 mm (70.9 in)

When planning for the installation, consider the space implications in your computer room for the possibility of adding more frames in the future.

- Weights[4]:
  - IBM 3584-L32 with 1 drive, no cartridges: 423 kg (932 lb.)
  - IBM 3584-L32 with 12 drives, 227 cartridges: 570 kg (1256 lb.)
  - IBM 3584-D32 with no drives, no cartridges: 355 kg (784 lb.)
  - IBM 3584-D32 with 12 drives, 396 cartridges: 558 kg (1229 lb.)

8.5.2 Floor requirements

Install the library on a raised or solid floor. The floor must have a smooth surface and, if raised, must not have ventilation panels beneath the leveling jackscrews. If carpeted, ensure that the carpet is approved for computer-room applications. To accommodate unevenness in the floor, you can raise or lower the leveling jackscrews to the following specifications:

- Maximum allowable variance must not exceed 7 mm (0.27 in) per 76 mm (3 in).
- Maximum out-of-level condition must not exceed 40 mm (1.6 in) over the entire length and width of the library.

The floor on which the library is installed must be able to support:

- Up to 4.8 kilograms per square cm (68.6 lb per square inch) of point loads exerted by the leveling jackscrews
- Up to 211 kilograms per square meter (43.4 lbs per square foot) of overall floor loading

The number of point loads exerted depends on the number of frames that make up the library. There are four point loads per frame (located at the corners of each frame).

[4] The weight with cartridges assumes a cartridge weight of 0.209 kg (0.460 lb) for a standard cartridge. The actual weight of the library varies, depending on the configuration and cartridge capacity.

10561
A-

8.5.3 Operating environment

The IBM 3584 is designed to operate in the following environment:

- Temperature: 16° to 32° C (61° to 89° F)
- Relative Humidity: 20% to 80%
- Wet Bulb: 23° C (73.4° F) maximum

8.5.4 Power and cooling specifications

Power and cooling for the IBM 3584 components are provided by the housing frame. Each base and expansion frame that contains drives has its own frame control assembly (FCA), which receives power from a customer-supplied outlet and, in turn, provides AC power to all tape drives within the frame. The FCA for the L32 contains two DC power supplies; actually, only one DC power supply is needed to operate the entire library. Before support was provided for 16-frames, all additional FCAs in D32s included one additional DC power supply for redundancy. With support for 16-frames, the additional FCAs in the D-Frames no longer have a default-installed DC power supply.

Additional DC power supplies can nevertheless be ordered or made available for extra frames, as explained in 8.2.2, "Library control systems: frame control assembly" on page 167.

The FCA is not required in expansion frames that contain no tape drives.

Each frame receives single-phase (200-240 V ac) power on its own power cord from a customer-supplied outlet. Certain countries or regions require two-phase power to achieve the 200-240 V ac required by the frame. Countries in North America have the option of operating at 100-127 V ac power (FC 9951).

A new Dual AC Power feature (FC 1901), supporting either 110 V ac or 220 V ac, is available for the IBM 3584, providing two independent line cords that may be connected to two independent customer branch circuits. A power switch connects to one of two customer power feeds and passes all AC power to the frame from that feed. The switch monitors the AC line voltage from the feed it is using and automatically switches to the alternate AC power feed if the incoming voltage drops below a preset level.

Table 8-6 on page 192 lists the power requirements for the L32 and D32 frames.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1356
3698
Doc.

Table 8-6 Power requirements for the IBM 3584

Power requirement	Model L32 or D32	
	220 V ac line cord	110 V ac line cord
AC line voltage	200 to 240 V ac (nominal)	100 to 127 V ac (nominal)
AC line frequency	50 to 60 Hz	50 to 60 Hz
Nominal power	1.4 kW	1.2 kW
Line current	8.0 A	12.0 A
kVA	1.6 kVA	1.2 kVA
Heat output	4.8 kBtu/hr	4.1 kBtu/hr
Inrush current	200 A (peak for 1/2 cycle)	100 A (peak for 1/2 cycle)

Note: Values shown for frames with 12 IBM LTO Ultrium tape drives installed.

8.6 Host platforms and device drivers

The IBM 3584 is supported on many operating systems. For a current list of host software versions and release levels that support the 3584, refer to:

`http://www.storage.ibm.com/tape/lto/3584/3584opn.pdf`

The following no-charge specify codes indicate the server platform to which the IBM 3584 is attached. These features are used by IBM for device driver distribution:

- Feature #9210, attached to HP-UX
- Feature #9211, attached to Sun System
- Feature #9212, attached to Windows System
- Feature #9213, attached to other non-IBM system
- Feature #9215, attached to Linux System
- Feature #9400, attached to iSeries System
- Feature #9600, attached to pSeries

You are not limited to one platform-attach feature as the library may be attached to more than one of these platforms. You cannot add more than one of each feature; in other words, if you have two or more Windows servers, only one feature #9212 is required. The device driver will be delivered on a CD that contains all available device drivers for each OS and the documentation.

10559
A.

Tip: The device driver CD or diskette that is shipped with the IBM 3584 may not contain the most recent device drivers. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

8.6.1 Device driver installation

Install the IBM device drivers for the IBM 3584 as follows:

- If you intend to use the IBM 3584 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3584.
- If you do not intend to use the IBM 3584 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide*, GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3584 with a commercial software application, IBM recommends that you install any IBM-supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

8.7 Storage applications

Software to exploit the IBM 3584 is not provided with the library. Additional software support is available through products that must be obtained separately from IBM, IBM Business Partners, or independent software vendors. A list of compatible software is available at:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1 and Ultrium 2 support and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more information about specific versions and platforms supported. Many examples of third-party software applications with IBM LTO drives and libraries are given in the Redbooks *Implementing IBM LTO in*

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls 1357
Nº Doc 3698

Linux and Windows, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

8.8 IBM 3584 initial setup

The following sections cover some of the major items required to implement, manage, and operate the IBM Ultrium tapes and libraries. We do not cover all tasks, and we do not intend to cover all of the specific commands. For more details, refer to the *IBM 3584 UltraScalable Tape Library Planning and Operator Guide*, GA32-0408.

8.8.1 SCSI ID

The IBM 3584 uses multi-path architecture, so it has no direct SCSI connection to a host system. When the host communicates with the library, it must send the communication via a control path to a drive designated as LUN 1. A control path is the drive SCSI port through which a host system sends its commands to a logical library within the IBM 3584. (Refer to 2.6, "Multi-path architecture" on page 46 for an explanation of the concept of logical libraries.) When you add multiple control paths to the IBM 3584 library, any single, configured logical library can be accessed by multiple host systems.

Additional control paths also reduce the possibility that failure in one control path will cause unavailability of the entire library.

Note: The setup and SCSI configuration of the IBM 3584 are usually performed by an IBM service representative.

8.8.2 Element number

Element numbers identify the physical location within the library. This information is required mostly for storage applications, such as IBM Tivoli Storage Manager, which translate the device to a name that the robotic understands.

In the IBM 3584, each SCSI storage element is assigned a SCSI element address. A SCSI storage element is a physical location capable of holding a tape cartridge (such as an I/O slot, drive, or storage slot). The element numbering is split into three sections:

- The tape drive sequence
- The I/O station sequence
- The cartridge slot sequence

10557
A.

Note: The numbering is contiguous for the cartridge slot sequence. However, the addition, removal, or movement of one or more tape drives affects the element numbering of the cartridge slots.

Table 8-7 shows the element numbers for tape drives in each IBM 3584 frame up to six frames. For element numbers up to the maximum 16 frames, see the *IBM TotalStorage UltraScalable Tape Library Planning and Operator Guide*, GA32-0408.

Table 8-7 IBM 3584 tape drive element numbers

Drive number	Frame 1 (L32)	Frame 2 (D32)	Frame 3 (D32)	Frame 4 (D32)	Frame 5 (D32)	Frame 6 (D32)
1	257	269	281	293	305	317
2	258	270	282	294	306	318
3	259	271	283	295	307	319
4	260	272	284	296	308	320
5	261	273	285	297	309	321
6	262	274	286	298	310	322
7	263	275	287	299	311	323
8	264	276	288	300	312	324
9	265	277	289	301	313	325
10	266	278	290	302	314	326
11	267	279	291	303	315	327
12	268	280	292	304	316	328

Each element in the IBM 3584 (the cartridge storage slots, I/O storage slots, and tape drives) has two addresses:

- Physical address
- SCSI element address

When initiating an operation such as moving a tape cartridge or performing manual cleaning, you can use the physical or logical address to specify a location in the library.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1358
3698
Doc.

The physical address consists of frame, column, and row identifiers that define a unique physical location in the library. The address is represented as:

- Fx,Cyy,Rzz for a storage slot (where F equals the frame and x equals its number, C equals the column and yy equals its number, and R equals the row and zz equals its number).
- Fx,Rzz for a tape drive and I/O storage slot (where F equals the frame and x equals its number, and R equals the row and zz equals its number).

The SCSI element address consists of a bit and hex value that defines to the SCSI interface a logical location in the library. This logical address is represented as xxxx (X'yyy'), where xxxx is a bit value and yyy is a hex value. It is assigned and used by the host when the host processes SCSI commands. The SCSI element address is not unique to a storage slot, drive, or I/O slot; it varies, depending on the quantity of drives in the library.

For example, the storage slot address F2,C03,R22 means:

- F2: frame 2 (first expansion frame)
- C03: column 3 (second column from left on drive side)
- R22: row 22 (22nd position down from the top of the column).

Each drive has a unique address to indicate its physical location. The drive address consists of two values, a frame number and a row number:

- Frame number: Represented as Fx, where F equals the frame and x equals its number. Regardless of whether any drives are installed, the frame number for the base frame is 1 and increments by one for each adjacent expansion frame.
- Row number: Represented as Rzz, where R equals the row and zz equals its number. The row number is 1 for the top drive position in the frame, and increments by one for each row beneath the top drive. Regardless of whether drives are installed, the row numbering is the same for every frame.

A drive address of F2,R10 means frame 2 (that is, the first expansion frame), row 10 (10th drive position from the top of the column).

8.9 Operator displays and buttons

The IBM 3584-L32 operator display is a touch screen with integrated touch buttons. The display default setting will return to the basic main menu after five minutes of inactivity. The screen has three sections (Figure 8-19 on page 197):

- The menu title and panel number
- The informational section
- The selectable buttons

10555
A.

Navigate through the operator panels by pressing the touch screen buttons:

- BACK:
  Will take you back to the previous screen. You may need to press the BACK button several times to return to the main status screen.
- UP and DOWN:
  If you are on a menu panel, these keys will navigate up and down within the current panel, scrolling one line when pressed once. If you keep the UP or DOWN keys pressed, scrolling will speed up. The longer you hold the keys, the faster will the scrolling be.

  If you are selecting a value, the keys will increment or decrement the value.
- ENTER:
  The selected item is shown using reverse video. No action is processed until the ENTER key is pressed.

The default display is the Activity Status Display. The information in the Activity screen is replaced automatically by an error message whenever the Ultrium tape library detects that:

- A permanent error has occurred.
- A drive requires cleaning, and automatic cleaning has been enabled.
- A drive requires cleaning, and no cleaning cartridge is present in the library.

Figure 8-19 IBM 3584-L32 operator display

Other commands or options will appear on various screens. From the main activity screen, you can access the Library Main Menu by pressing the MENU key, or pause the library for maintenance operation with the PAUSE key.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1359
Doc. 3698

The PAUSE key causes the library to park the cartridge accessor in an area that gives clear access to the library's interior (if you need to open the front door). If you accidentally press the PAUSE key, wait for the 30-second time-out. The library will automatically resume operation.

Attention: If you press the PAUSE key, then open the front door, the library rejects requests for new operations.

When selecting a critical command, such as pressing the PAUSE key, a confirmation screen will be displayed. You will see a text message with two keys, CONTINUE and CANCEL. The CONTINUE key will proceed and execute your command, and the CANCEL key will return to your previous screen.

The screens on the operator panel fall into six categories:

- Library status:
  Provides information about the accessor, the cartridge locations, the drives, and the slots.
- Manual operations:
  Enables manual intervention such as cartridge movements, cleaning, and inventory.
- Settings:
  Displays and changes configuration set-up variables such as cleaning mode, date, enabling/disabling of drives, and virtual library configuration.
- Statistics:
  Reports usage information about the accessor, drives, and cleaning cartridges.
- Vital Product Data (VPD):
  Describes the library, drives, and accessor.

  This includes such information as the machine types, model numbers, serial numbers, and the level of firmware.
- Service:
  Places the library into service mode for repairs or upgrades to be carried out.

8.10 Sequential versus random access

The IBM 3584 is designed to operate only in random mode under the control of a storage application. Sequential mode is not supported.

10553
A.

9

IBM xSeries LTO tape products

The xSeries Family of servers also features IBM Ultrium Libraries. Designed for tape automation, the IBM 3607-26X Autoloader and IBM 4560SLX Tape Library can be attached to xSeries servers and other Intel/Windows servers. They use the LTO Ultrium tape drives for faster data transfer and reliability in automated library service.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1360
3698
Doc

9.1 IBM 3607-26X and 4560-SLX

Figure 9-1 IBM 3607-26X Autoloader

The IBM 3607-26X Autoloader houses one Ultrium 1 tape drive with a native data transfer rate of 15 MBps and a cartridge capacity of 100 GB. The drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm, which provides an effective data rate of up to 30MBps and a cartridge capacity of up to 200 GB (with 2:1 compression) on Ultrium 1 media.

The IBM 3607-26X has one I/O slot and a cartridge capacity of 16 slots, allowing a native capacity of 1.6 TB of uncompressed data. With compression (assuming 2:1), the 3607-26X can store 3.2 TB of data.

The IBM 3607-26X Autoloader is an excellent high-performance, entry-level choice for small to midrange systems.

Table 9-1 3607-26X Autoloader model summary

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	Ultrium 1 tape drives
3607-26X	16[a]	1.6 TB	3.2 TB	1

a. Plus one (1) I/O Station slot

10551
VA.

Figure 9-2 IBM 4560-SLX Modular Tape Library

The IBM 4560-SLX Modular Tape Library houses up to two Ultrium 1 tape drives in a module.

Ultrium 1 drives have a native data transfer rate of 15 MBps and a cartridge capacity of 100 GB. The Ultrium 1 drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm that provides an effective data rate of up to 30 MBps and a cartridge capacity of up to 200 GB (with 2:1 compression) on Ultrium 1 media.

The IBM 4560-SLX has one I/O slot and a cartridge capacity of 30 slots allowing a native capacity 3 TB of uncompressed data. With compression (assuming 2:1), the 4560-SLX can store 6 TB of data.

The IBM 4560-SLX provides excellent tape storage scalability for mid range to high-end xSeries systems. It is expanded by configuring additional modules with the Elevator Link Option and the Elevator Link Extension Option. These features allow the library to grow to eight modules in total. This provides a maximum slot capacity of up to 240 slots when all eight modular units are installed. The Elevator options allow the library to pass cartridges between the modules, increasing the number of slots.

Table 9-2 4560-SLX Modular Tape Library with Ultrium 1 drives

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	Ultrium 2 tape drives
4560-SLX	30[a]	3TB	6TB	2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1361
Doc 3698

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	Ultrium 2 tape drives
4560-SLX with one expansion module	60	6TB	12TB	4
4560-SLX with seven expansion modules	240[b]	24TB	48TB	16

a. Plus one I/O Station slot
b. Plus eight I/O station slots

9.1.1 Tape drives

The 3607-26X uses one LTO Ultrium 1 tape LVD drive. The 4560-SLX can use up to two Ultrium 1 tape LVD drives per module. The drive part number is:

- Ultrium 1 Drive - P/N 59P6658

If Fibre Channel connectivity is required for the 4560-SLX, a Fibre Channel Card Adaptor (P/N 59P6657) can be installed into the library.

Each Ultrium tape drive contains the electronics and logic for reading and writing data, control of the tape drive, management of the data buffer, and error recovery procedures. All tape drives are packaged as a common assembly that is a Field Replaceable Unit (FRU), designed for quick removal and replacement.

9.1.2 Barcode reader

A barcode reader is provided as standard with the 3607-26X and 4560-SLX, and it does not affect the slot capacity of the libraries. The barcode reader is used during the inventory process to locate all cartridges inserted in the library. This action is repeated every time the front door is opened to ensure that the inventory is updated if a cartridge has been manually added, moved, or removed while the door was open.

9.1.3 I/O station

This facility allows the insertion and ejection of cartridges without interrupting the normal operation of the library. There is a single-slot I/O station where a cartridge can be inserted or ejected by opening the I/O station door.

10549
A-

9.1.4 Robotic system

In conjunction with the library control microcode, the robotic system identifies and moves cartridges between the storage slots, tape drives, and the I/O station. It has several components:

- A cartridge picker for placing cartridges in storage slots, tape drives, or the I/O station
- A barcode reader used to set up the library initially when it identifies the types of media and tape drives installed in the library, and in normal operation for reading the external labels on the cartridges when it locates and categorizes all cartridges installed in the library
- X-axis and Z-axis drive motors for rotating the picker assembly, and moving it horizontally, inside the library enclosure

9.1.5 Library control and operation

The Library Control Unit contains the electronics and logic for autochanger and library operations. The Library Control Unit controls all operations in the library, including the interaction between the library and the operators. The control unit Licensed Internal Code creates and maintains the library configuration, the physical location of the robotic system, and the inventory of cartridges. The database is kept in the flash memory of the library control hardware.

Requests issued from the server result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges to and from the tape drives and for inserting and ejecting cartridges. The host has records of the physical location of a cartridge in the library, and the physical location is also managed by the library.

In addition to requesting movement of cartridges in the library, the host can obtain status, performance, and configuration information, as well as information about the cartridges stored in the tape library.

Each cartridge must have a machine- and operator-readable external barcode label to identify a media cartridge in the library during initial inventory and any time a cartridge is added to the library. The library stores the physical location of the cartridge in an inventory database based on the cartridge label. All host application requests for operations involving movement or use of a cartridge need only reference the physical location of the cartridge (using an element number as described in 9.9.1, "Identifying library locations element numbers" on page 207) for the library to perform the request.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1362
3698
Doc.

9.1.6 Operator panel

An LCD operator control panel on the front of the machine provides status information and menu options. From this panel the operator can initiate actions such as moving and loading tape cartridges or invoking diagnostics.

9.1.7 Maintenance

The cartridge storage slots, cartridge picker, and tape drives are accessed for maintenance purposes by opening the front door of the library. The tape drives, power supplies, and host interface board are accessed from the back of the library for maintenance.

9.2 Library options

The following part numbers can be used to order features for the libraries (Table 9-3). We have not included the various cabling options. Refer to the product publications for detailed information about configuring and ordering the IBM Libraries, or visit:

`http://www.pc.ibm.com/ww/eserver/xseries/tape.htm`

Table 9-3 IBM 4560-SLX options

Option	Description	Comment
59P6657	IBM Fibre Channel Card	Require either 59P1271 or 59P1272
59P6658	Ultrium 1 Drive	LVD Connection
59P6659	LTO Cartridge Magazine	Left and Right base magazines
59P6662	Elevator Link	Required when adding a second module
59P6663	Elevator Link Extension	Required when adding two or more modules
59P1271	Longwave GBIC	To be used in conjunction with 59P6657
59P1272	Shortwave GBIC	To be used in conjunction with 59P6657
49P3200	100GB Ultrium 1 Tape cartridge	

10547
A

Option	Description	Comment
35L2086	Universal LTO Cleaning cartridge	

There are no additional part numbers required for the 3607-26X except the data cartridge 49P3200 and the Universal LTO Cleaning Tape 35L2086.

9.3 Physical attachments

The 4560-SLX Modular Tape Library and 3607-26X Autoloader can be attached to IBM xSeries servers and other Intel/Windows servers that support the SCSI LVD and Fibre Channel interface. Refer to the latest compatibility matrix to determine which xSeries servers support the libraries:

`http://www.pc.ibm.com/us/compat/storage/tmatrix.html`

SCSI cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code should also be specified.

9.4 Cabling

A SCSI cable is required for each library connection to a SCSI bus. If no cable is available, one should be specified on the initial order for each library or drive. A SCSI terminator is included with each cable. An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) may also be required for attachment to particular server adapters.

Be sure to determine the exact SCSI connection type at the host to ensure that the correct cable connections are ordered, then determine the length from the host to the tape library.

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection. If using multi-drop interconnection, then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

For FC cables, there are only two connection types, LC and SC. Once the connection type is determined then only a correct length has to be determined.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1363
Doc: 3698

9.5 Environmental specifications

The physical dimensions for the 4560-SLX are:

- Width: 42.4 cm (16.7 in)
- Depth: 78.7 cm (31 in)
- Height: 22.2 cm (8.75 in) for a stand-alone library on casters
- 5 EIA units high (if rack-mounted)

The physical dimensions for the 3607-26Xare:

- Width: 44.7 cm (17.7 in)
- Depth: 70.3 cm (29.7 in)
- Height: 8.9 cm (3.5 in) for a stand-alone library on casters
- 2 EIA units high (if rack-mounted)

9.6 Storage applications

The software to manage the tape libraries is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software providers. Contact your vendor for information about support of xSeries tape products, or see the IBM ServerProven® Web site at:

`http://www.pc.ibm.com/us/compat/`

9.7 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each library drive order[1]. With the initial order, additional data and cleaning cartridges may be ordered as a part number.

- Part number 49P3200 provides a single Ultrium 1 Cartridge.
- Part number 35L2086 provides a single Ultrium Cleaning Cartridge.

After the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor.

`http://www.storage.ibm.com/media/index.html`

Refer to Appendix A, "LTO Ultrium tape media" on page 223, for details about ordering supplies and cartridges, with or without labels.

[1] All media and cleaning cartridges are warranted separately from the IBM 3580 Ultrium tape drive.

10545
A

9.8 Installation and performance considerations

Installing more than one Ultrium drive on a SCSI bus may affect tape drive performance. For optimal performance, it is recommended that no more than one IBM Ultrium drive be attached to an individual SCSI bus.

While the IBM Ultrium tape drives provide the capability for high tape performance, other components of the system may limit the actual performance achieved. The compression technology used in the tape drive can typically double the amount of data that can be stored on the media; however, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

9.9 Library features

The following section covers some of the major items required to implement, manage, and operate the IBM tape libraries. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the manual for your library listed in Table 9-6, "Library manuals" on page 211.

9.9.1 Identifying library locations element numbers

To manipulate the media within the library, the host must reference each movement with source and target designations. This is done via element addressing, which specifies precisely which slots within the library are to be used. Table 9-4 shows the element addressing scheme used for the 4560-SLX tape library.

Table 9-4 IBM 4560-SLX element numbering

Column	Element numbers
Picker	0
I/O station	448
Drives	480-481
Storage	32-58

Table 9-5 on page 208 shows the element addressing scheme used for the 3607-26X tape library.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1364
Doc. 3698

Table 9-5 IBM 3607-26X element numbering

Column	Element numbers
Picker	0
I/O station	N/A
Drives	32
Storage	256-271

9.10 Operator displays and buttons

Normally, the host issues commands to the tape library. Operator control is provided via the Operator Panel. The operator is responsible for:

- Starting the tape library
- Shutting down the tape library
- Handling media

Refer to the manual for your library, listed in Table 9-6, "Library manuals" on page 211, for your library for media handling procedures. In the case of equipment failures, the operator can perform media processing.

9.10.1 Operator panels

Figure 9-3 and Figure 9-4 on page 209 show the operator panels for the 3607-26X and 4560-SLX respectively.

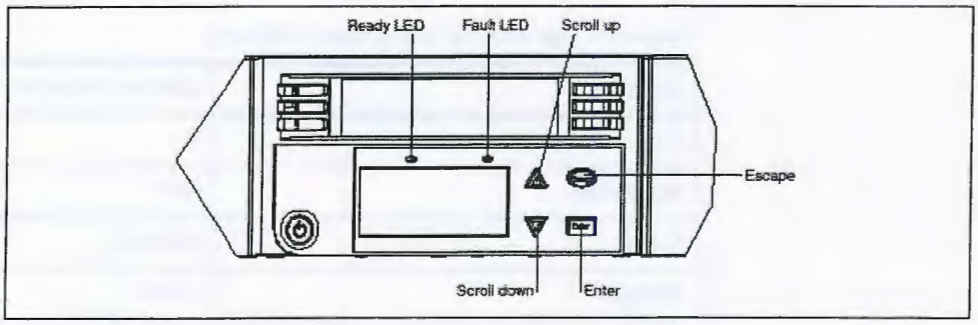


Figure 9-3 3607-26X front panel

10543
A.

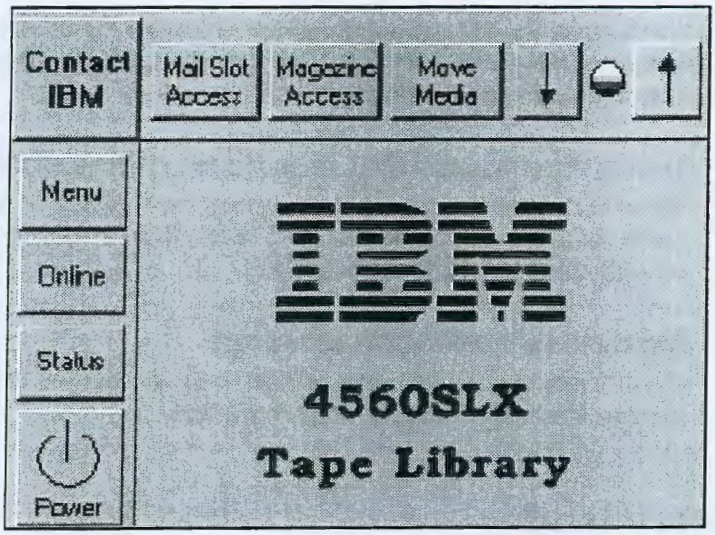


Figure 9-4 4560-SLX touch screen front panel

The operator panel provides communication between the operator and the IBM tape library. Visual indications and push buttons enable the operator to control the tape library.

1. I/O Station status:
   The I/O Station status area provides constant information about the I/O Station.
2. Library status:
   The library status area displays information such as online or offline status, library reports status, and messages to solicit operator intervention.
3. Messages:
   The display communicates interactive dialogs, special messages, alerts, and library configurations. More details are covered in the operator manual.
4. Drive status:
   The drive status area provides constant information about the drives, such as:
   - Presence of tape drive (illustrated by a black outline box for each drive)
   - Power to the tape drive
   - Cleaning requirements
   - Compression
   - Write protection
   - Tape activity

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1365
Doc. 3698

9.10.2 Menu options

Each menu is accessible through the Operator Panel push buttons. For the actual menus for your library, refer to the manual for your library listed in Table 9-6, "Library manuals" on page 211.

Using commands that require an offline state

Some commands require that the library be in an offline state. If any such commands are attempted while the library is in an online state, the operator will be requested to take the library offline.

Operator intervention message

If a problem causes an operator intervention message to appear, refer to the messages section of your operator manual.

9.11 Library modes

The libraries operates in either base or random access mode. The Library Mode will be determined by the application software managing your library.

9.12 Drive cleaning

All IBM Ultrium Tape Drives have an integrated cleaning mechanism which brushes the head at load time and again when unloading a cartridge. The drives also have a cleaning procedure that uses a special cleaning cartridge, should this become necessary.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

With each library, a specially labeled IBM LTO Ultrium Cleaning Cartridge is supplied to clean the drive head. The drive determines and alerts you when the head needs to be cleaned. Refer to the operations manual for details for Automatic Cleaning or Manual Cleaning.

9.13 Firmware upgrades

Each IBM Ultrium tape drive and tape library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, make sure the current

firmware is installed on your IBM LTO tape drives and library. As the libraries are designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed. Determine the latest level of firmware available by visiting `http://www.pc.ibm.com/` or by contacting the IBM Call Center.

Follow the instructions for updating your firmware in the operator manual for your library. Table 9-6 shows the various manuals available for the xSeries LTO products.

Table 9-6 Library manuals

Manuals	Part numbers
1x16 Autoloader Quick Start Guide	71P9131
1x16 Autoloader User's Guide	46P3206
4560SLX Tape Library Quick Installation Guide	59P6702
4560SLX User's Guide	59P6690
Fibre Channel Option Card Users Guide	59P6748

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1366
Doc 3698

10540
A.

10

LTO and iSeries considerations

This is a short overview and update about installation and implementation of LTO Tape Drives and LTO Tape Libraries for iSeries.

A redbook and Redpaper address this topic:

- *iSeries in Storage Area Networks*, SG24-6220
- *The LTO Ultrium Primer for IBM @serveriSeries Customers*, REDP3580

However, these publications cover only LTO Ulrium 1, so we will provide updates and additional information.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1367
3698
Doc.

10.1 iSeries support for IBM LTO Ultrium 2

IBM LTO Ultrium 2 tape drives are supported on RISC machines with OS/400 V5R1 and later.

The following PTFs are needed:

- V5R1 SI07884
- V5R2 SI07885

These PTFs fix a problem with the INZTAPcommand when using LTO 1 and 2 media in the same library.

Tip: *Info APARs*, periodically issued by IBM, contain important information about iSeries topics. There are currently two Info APARs about LTO: II12621 for Ultrium 1 and II13513 for Ultrium 2. These are available in the PTF database, from the Web site:

`https://techsupport.services.ibm.com/server/support?view=iSeries`

Look in the Find it Fast column, and choose Search Technical Databases. Leave the box at the top set at Search APARs, and click **Go**. Enter the Info APAR number in the search box and click **Search**.

You will need these V5R1 and V5R2 PTFs if you change the TAPF from its default density of *DEVTYPE. This is normally only done when using *NL tape label processing.

LTO 2 products can be attached to iSeries systems with any of these adapters:

- 6534 Magnetic Media Controller (SPD), HVD, HD68

  Up to 17 MBps (60 GBph)
- 2729 PCI Magnetic Media Controller, HVD, HD68

  Up to 13 MBps (47 GBph)
- 2749 PCI Ultra Magnetic Media Controller IOA, HVD, HD68

  Up to 38 MBps (108 GBph)
- 5702 Ultra160 SCSI IOA PCI-X Ultra Tape Controller, LVD, VHDCI

  Up to 70 MBps (250 GBph)
- 2765 FC IOAPCI Fibre Channel Tape Controller

  Up to 95MBps (340 GBph)

10538

LTO 2 SCSI drives are supported with multiple drives connected to a single adapter (daisy-chained) for either the LVD or HVD adapters. The LTO 1 drives are still limited to a single-drive configuration.

The following restrictions apply:

- No support for LVD SCSI LTO 1 products on the 5702 adapter
- No 6501 support for LTO 2

There is no performance increase with the HVD SCSI attached LTO 2 devices. Performance is limited by the HVD SCSI interface.

10.2 BRMS and LTO tape libraries

Both LTO 1 and LTO 2 drives can be in the same logical library and share a common inventory *but* you must not attach both drive types to the same I/O adapter. They must be separated at the adapter level for OS/400 to pool the drives together properly.

At the time of writing, OS/400 will show both the LTO 1 (L1 media type) and LTO 2 (L2 media type) as *L* so the user will not be able to determine from the WRKTAPCTG screen which cartridges are of which type.

OS/400 will NOT filter out the LTO 2 cartridges from the LTO 1 MLB so it is up to the user to manage the cartridges using BRMS media classes. The LTO 1 cartridges will have to be added to media class ULTRIUM1, and LTO 2 tapes will have to be added to media class ULTRIUM2. Attempting to use an LTO 2 cartridge in a LTO 1 drive will result in a failure.

For LTO 1 drives the density *CTGTYPE will result in *ULTRIUM1 for LTO 1 cartridges, and the density *DEVTYPE will result in *ULTRIUM1. LTO 2 cartridges are not supported in LTO 1 drives.

For LTO 2 drives the density *CTGTYPE will result in *ULTRIUM1 for LTO-1 cartridges and *ULTRIUM2 for LTO 2 cartridges. The density *DEVTYPE will only work for the LTO 2 drive with LTO 2 media, the device's highest capability.

RQS nº 03/2005 - CN
CPMI CORREIOS
1368
Fls Nº
Doc. 3698

10.3 iSeries resources

The iSeries can control drives and libraries through CL commands and APIs or through software such as BRMS/400. For V4R4 and later, LTO devices report as:

IBM 3580

- 3580 tape drive:
  - Resource -> 3580, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 002

IBM 3581

- 3581 tape drive:
  - Resource -> 3581, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 002
- 3581 Autoloader unit:
  - Resource -> 3581, Device Description -> TAPMLBxx (xx=01, 02, 03, etc.)

When the IBM 3581 is in random mode and an IPL is run for the system or IOP, a TAPMLBxx and TAPxx resource will be created. If the drive is in sequential mode and an IPL is run for the system or IOP, then only a TAPxx resource will be created (that is, the TAPMLBxx will be removed). If the drive normally is used in random mode, it can be changed to sequential mode. In this case, de-allocate the tape resource from the WRKMLBSTS command screen and vary on the tape drive to use as a standalone drive. Make sure the system has not run an IPL before changing the drive back to random mode. If the autoclean function is enabled or disabled, the IOP or IOA must run an IPL before using the 3581 device.

If the barcode feature is installed, the device is in random mode, and the drive is powered up with a cartridge loaded, the loaded cartridge will be missing when a WRKTAPCTG command is run on the iSeries. The cartridge has to be unloaded and the library re-inventoried to show the cartridge. If the 3581 is to be used as an alternate IPL device (as in a D Mode IPL), set the SCSI address on the tape device to 0.

Unloading volumes on IBM 3581

When using the 3581 device in sequential mode, if a user selects the option Load Slot and SRC Slot to mount a volume in the drive (when using tape commands CHKTAP, DSPTAP, INZTAP, SAVxxx, with the ENDOPT(*UNLOAD)), the cartridge will eject from the drive but will not be returned to a slot. For this to happen, the user must specify SEQ START. Loading a slot is a manual operation and the autoloader will not return the cartridge, so it must be unloaded as it was loaded from the panel. The autoloader operation must be *started* to get the cartridges loaded and unloaded.

10536
A-

IBM 3582

- IBM 3582 tape drives:
  - Resource -> 3582, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 002
- IBM 3582 Robotic:
  - Resource -> 3582, Device Description -> TAPMLBxx (xx=01, 02, 03, etc.)
  - 3582 023 with 3580 002 drives

IBM 3583

- IBM 3583 tape drives:
  - Resource -> 3583, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 001 and 3580 002
- IBM 3583 Robotic:
  - Resource -> 3583, Device Description -> TAPMLBxx (xx=01, 02, 03, etc.)
  - 3583 0xx with 3580 001 and 3580 002

3583 with SDG Fibre Channel limitations

The 3583 device with FC 8005 (Fibre Channel attach) uses only LVD SCSI drives. V5R1 and later have Fibre Channel support. All FC attachments must be direct attached or homogeneous zones with iSeries only. The 3583 FC attached library has two Fibre Channel ports. The device can be shared with other platforms but it is strongly recommended that each platform be connected to separate ports. If zoning is used in the SAN device, be sure that the all iSeries hosts have a connection to the media changer. All six tape devices can be used but performance must be considered with the larger configuration. Alternate IPL is not supported for Fibre Channel attached tape devices. The Alternate Install Device (Boot Manager) must be used instead.

3583 non-multi-path architecture Fibre Channel recommendations

When sharing the 3583 FC with two or more hosts concurrently it may fail if the default time out for the *initial mount wait time* and the *EOV mount wait time* is used. These values have to be increased to a suggested 5-10 minutes. In general, larger library configurations and shared configurations tend to get a time-out error, so increasing this value is required.

IBM 3584

- IBM 3584 Tape drives:
  - Resource -> 3584, Device Description -> TAPxx (xx=01, 02, 03 etc.)
- IBM 3584 Robotic:
  - Resource -> 3584, Device Description -> TAPMLBxx (xx=01, 02, 03 etc.)
  - 3584 032 with 3580 001 and 3580 002 drives

Note: The Problem Analysis Log (PAL) will show 63A0 and 9429.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1369
Doc. 3698

Fibre Channel limitations

For V5R1, the iSeries Fibre Channel 3584 support is limited to a single-drive configuration per adapter. Multiple systems may share a drive with the use of a 3534 Hub or 2109 switch. If the 2109 switch is used it must be set to Quick Loop mode for the ports used on the iSeries. Each system or LPAR may have multiple drives but each drive requires an adapter. Each drive connection must have a library control path enabled.

Alternate IPL is not supported for Fibre Channel attached tape devices.The Alternate Install Device (Boot Manager) must be used instead.

10.3.1 Configuration changes

If making any configuration changes on LTO drives and libraries you must run an IPL on the IOA/IOP on the iSeries.

10.4 OS/400 V5R1 restriction for multi-path architecture libraries

The IBM 3582, 3583, and 3584 feature multi-path architecture. Unlike other platforms, the iSeries requires a dedicated control path for each iSeries drive. This is true for both SCSI and fibre drives for OS/400 V5R1. This is not the way the library is shipped, so you have to enable the control paths on all drives that are connected to an iSeries. You can do this either on the operator panel or with StorWatch. If you forget to do this, the drives will not autoconfig properly.

If you have configured your library properly, then you will see as many tape libraries in OS/400 as there are tape drives are assigned to your server. For example, if you have a 3584 with three drives assigned to the iSeries, then you see three TAPMLBxx (TAPMLB01, TAPMLB02, TAPMLB03), each with three TAPxx (TAP01, TAP02, TAP03).

10.5 OS/400 V5R2

Version 5 Release 2 includes support for multiple targets from a single Fibre Channel tape or disk adapter. Before this release, only a single target was supported from an initiator (FC adapter). Up to 16 LUNs are supported. A target is a physical tape drive. In the case of tape this means a single-tape FC adapter can support multiple tape devices. For example, with V5R1, if you had four iSeries with four FC tape devices, sixteen FC tape adapters would have been required to enable all iSeries to address all tape devices, as each FC adapter is

10534
A.

allowed to see only one target. At V5R2 this number is reduced to four, one FC tape adapter per iSeries because each FC adapter may see multiple targets. This is illustrated in Figure 10-1. In summary, LTO 2 and V5R2 FC allow multiple device configurations per adapter and therefore one control path per adapter is required.

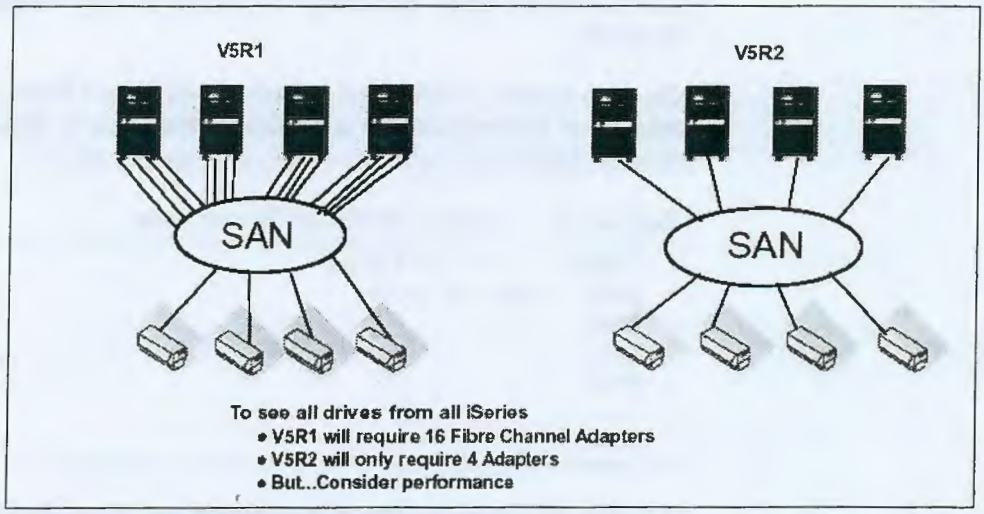


Figure 10-1 Multiple-target support

A maximum of 16 tape LUNs may be addressed from a single iSeries tape FC adapter. A LUN is a tape device or media changer. So in the case of a 3583 LTO tape library, which may have six drives and a media changer, seven LUNs will be reported. This example dramatically decreases the cost of hardware required to support multiple devices from multiple iSeries, but there are other considerations, such as management of tape devices.

Sharing the devices requires only a standard **`vary on`** and **`vary off`** command. When the iSeries varies on a tape it will use a *reserve* lock on the tape device to prevent other systems from using the drive. However, in a heterogeneous setup other operating systems may also share the drive. A benefit of the iSeries is its ability to *reserve/release* a tape drive. This prevents other systems writing to the middle of a tape in use by an iSeries and ensures tape data integrity for iSeries users. The same may not be true for other operating systems, and therefore it is entirely possible for an iSeries to start using a tape drive in use by another system. You will have to check with each vendor to establish whether they support *reserve/release* of a tape drive.

Tape management software such as BRMS and IBM Tivoli Storage Manager use the *reserve* lock. For other packages, check with the software vendor.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1370
Doc 3698

10.6 Tape drive sharing and management

OS/400 is an integrated operating system, so all device management function is included, with no extra software required for drive allocation and automation. This function simplifies drive sharing, especially when fibre drives are used, and all hosts can see all drives. This section shows how it works; it is the same for both SCSI and fibre drives, but using fibre drives is more flexible, as more drives are available.

On each system, OS/400 will autoconfigure a tape library, and will find all of the drives that are inside it that are visible to the system. To see this, use the WRKMLBSTS command, as shown in Example 10-1.

Example 10-1 Output of WRKMLBSTS command

```
TAPMLB01  <<<<< the library
TAP01   <<<<< the drives
TAP02
TAP03
TAP04
 .....
TAPxx
```

For each drive you have to set the options that are at the top of the WRKMLBSTS command screen. You have three options:

- ALLOCATED: means that ONLY the system where it is allocated can use it.
- DEALLOCATED: means the system you are looking on CANNOT use it.
- UNPROTECTED: means that the drive will sit in limbo waiting for a system to use it. That system will use it, then put it back into *limbo* ready for the next system to use it.

For drive sharing, you would set all drives to UNPROTECTED status. This is the most common setup, especially on fibre.

When backing up with BRMS, just tell BRMS to save to TAPMLB01. BRMS will find a tape, find a drive, and run the save. If doing parallel saves, BRMS will get multiple drives running at once. You can also submit multiple jobs to get multiple drives running at once. And if all of the drives are busy and you submit another job, OS/400 will hold the new job on the library manager resource queue until a drive becomes available. Note that in order for this to work well, you will need to use CHGDEVMLB to increase the timeout parameters on the Initial Volume Mount Wait and End of Volume Mount Wait times. The defaults are 10 minutes, whereas 8 hours or similar is recommended for Initial Volume Mount Wait. If you have some saves that are higher priority than others, you may want to adjust the order you start them up, to make sure the critical ones get the drives first. If you

10532
A.

make a mistake, then within each system, OS/400 will prioritize the jobs on the library manager resource queue, and at the next tape mount, it will swap out the job that was running, and move in the job with the higher tape resource priority.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1371
Doc. 3698

10531
A

A

LTO Ultrium tape media

When an IBM 35XX Ultrium tape device is ordered, it will be supplied with one Ultrium data cartridge and one cleaning cartridge at no charge. Each member of the IBM 35XX Ultrium LTO family has different media features and rules that apply when placing the order. The following informationwill assist you in ordering additional media.

You can obtain tape cartridge supplies for use with the IBM LTO Ultrium 1 product family in three ways:

- Order features from IBM that are available only with the initial hardware order as described in "Features available with IBM LTO hardware initial order" on page 225.
- Order the IBM LTO Ultrium 1 media product offering (using a dummy IBM model type, 3589) as described in "IBM 3589 Ultrium 1 tape cartridge model number" on page 228.
- Contact the IBM MEDIA business supplies or a third-party supplier as described in "IBM media business distributors and other suppliers" on page 231.

You can obtain tape cartridge supplies for use with the IBM LTO Ultrium 2 product family in two ways:

- Order features from IBM that are available only with the initial hardware order as described in "Features available with IBM LTO hardware initial order" on page 225.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1372
3698
Doc

- Contact the IBM MEDIA business suppliers or third-party suppliers as described in "IBM media business distributors and other suppliers" on page 231.

Each of the following *additional media* features for Ultrium 2 will supply data cartridges with barcode labels that are not fixed to the data cartridges. The barcode labels will have be physically attached and the actual value of barcode labels cannot be pre-determined. For cartridges with fixed barcode labels and pre-determined barcode values, it is recommended that the media always be ordered through 1-800-IBM-MEDIA (refer to "IBM media business distributors and other suppliers" on page 231).

The media suppliers may supply tape cartridges from different manufacturers or offer a choice of brands. The tape cartridges you use must be manufactured by a qualified LTO media company to meet the LTO standards.

10529
A.

Features available with IBM LTO hardware initial order

The following media features are available for inclusion with the initial hardware order.

IBM TotalStorage Ultrium 1 Tape Drive 3580

These chargeable features provide media with the IBM 3580 Ultrium 1 tape drive and are available only with the initial order:

- Feature #8001 provides a single 100 MB Ultrium data cartridge with an unattached barcode label.

  A maximum of five is allowed.

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of three is allowed.

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with a barcode are included as standard with each initial order[1].

IBM TotalStorage Ultrium 2 Tape Drive 3580

These chargeable features provide media with the IBM 3580 Ultrium 2 tape drive and are available only with the initial order:

- Feature #8101 provides a single 200 MB Ultrium data cartridge without an attached barcode label.

  A maximum of 20 is allowed.

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of five is allowed.

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with a barcode are included as standard with each initial order.

IBM TotalStorage Ultrium Tape Library 3582

These chargeable features provide media with the IBM 3582 tape library and are available only with the initial order:

- Feature #8001 provides a single 100 MB Ultrium data cartridge.

  A maximum of 19 is allowed.

[1] Note that all media and cleaning cartridges are warranted separately from the IBM 3580 tape drive hardware.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1373
Doc 3698

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of three is allowed.
- Feature #8110 provides a pack of twenty 100 MB Ultrium data cartridges with unattached barcode labels.

IBM TotalStorage Ultrium 1 Scalable Tape Library 3583

These chargeable features provide media with the IBM 3583 Ultrium 1 tape library and are available only with the initial order:

- Feature #8001 provides a single 100 MB Ultrium data cartridge.

  A maximum of 19 is allowed.
- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of three is allowed.
- Feature #8010 provides a pack of twenty 100 MB Ultrium data cartridges with unattached barcode labels.

  The maximum allowed for different model types is shown in Table A-1.

Table A-1 Maximum number of media features for IBM 3583 Ultrium 1

IBM 3583 model	#8007 (cartridge cells)	#8010 (maximum allowed)
L18	0	1
L18	1	2
L18	2	3
L36	0	2
L36	1	3
L72	not applicable	4

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with barcode are included as standard with each initial order[2]

[2] Note that all media and cleaning cartridges are warranted separately from the IBM Ultrium hardware.

10527
A.

IBM TotalStorage Ultrium 2 Scalable Tape Library 3583

These chargeable features provide media with the IBM 3583 Ultrium 2 tape library and are available only with the initial order:

- Feature #8101 provides a single 200 MB Ultrium data cartridge without barcodes.

  A maximum of 19 is allowed.

- Feature #8110 provides a pack of twenty 200 MB Ultrium data cartridges without barcodes.

  The maximum allowed for different model types is shown in Table A-2.

Table A-2 Maximum number of media features for IBM 3583 Ultrium 2

IBM 3583 model	#8007 (cartridge cells)	#8110 (maximum allowed)
L18	0	4
L18	1	4
L18	2	4
L36	0	4
L36	1	4
L72	not applicable	4

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge without barcodes are included as standard with each initial order.

IBM TotalStorage Ultrium 1 UltraScalable Tape Library 3584

These chargeable features provide media with the IBM 3584 Ultrium 1 tape library frame models and are available only with the initial order:

- Feature #8750 provides a single Ultrium cleaning cartridge.

  A maximum of 10 is allowed.

- Feature #8757 provides a pack of twenty 200 MB Ultrium data cartridges without barcodes.

  The maximum allowed for different model types is shown in Table A-3 on page 228.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1374
Doc - 3698

Table A-3 Maximum number of media features for IBM 3584 Ultrium 1

IBM 3584 model type	#1603 (capacity expansion)	#8757 (maximum allowed)
L32 (base)	0	1
L32 (base)	1	1
D32 (expansion)	not applicable	1

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with barcode are included as standard with each initial Model L32 library order[2].

IBM TotalStorage Ultrium 2 UltraScalable Tape Library 3584

These chargeable features provide media with the IBM 3584 Ultrium 2 tape library frame models and are available only with the initial order:

- Feature #8767 provides a pack of twenty 200 MB Ultrium data cartridges without barcodes.

  The maximum allowed for different model types is shown in Table A-4.

Table A-4 Maximum number of media features for IBM 3584 Ultrium 2

IBM 3584 model type	#1603 (capacity expansion)	#8757 (maximum allowed)
L32 (base)	0	1
L32 (base)	1	1
D32 (expansion)	not applicable	1

IBM 3589 Ultrium 1 tape cartridge model number

You can use the IBM 3589 model number to order quantities of IBM LTO Ultrium 1 data and cleaning cartridges. Since this is not a true hardware machine type, engineering installation and maintenance are not relevant to it, no real serial number is applied to it (although cartridges have their own serial number types), and no MES features can be added to it once delivered.

Note there is no 3589 equivalent for Ultrium 2 tape cartridges.

10525
A

Model description

You may choose from three model types for the IBM 3589, where each model delivers a different cartridge specification:

- IBM 3589-004 provides Ultrium cleaning cartridges.

  Model 004 has a single chargeable feature, #4005, which indicates the required quantity of cleaning cartridges. Each feature delivers a pack of five cleaning cartridges. You must order at least one of these features for this model.

  The maximum allowed is six features per model order for a total of 30 cartridges; if you require more than 30 cartridges, order a second 3589 model 004 with additional features.

- IBM 3589-003 provides Ultrium 1 data cartridges with no labels.

  Model 003 has a single chargeable feature, #3020, which indicates the required quantity of unlabeled data cartridges. Each feature delivers a pack of 20 data cartridges. You must order at least one of these features for this model.

  The maximum allowed is 20 features per model order (400 cartridges); if you require more than 400, order a second model 003 with additional features.

- IBM 3589-002 provides Ultrium 1 data cartridges with a labeling service.

  Model 002 has a single chargeable feature, #2020, which indicates the required quantity of labeled data cartridges. As with the model 003, each feature delivers a pack of 20 data cartridges, and you must order at least one of these features for this model with a maximum of 20 features per model.

  However, in addition, you must order various no-charge features to indicate what volume serial range you want printed on the cartridge labels. The supplied barcode label is made up of 8 characters, a six-character VOLSER, and a two-character cartridge media-type identifier (L1), which identifies the cartridge as an LTO cartridge (L) and indicates that the cartridge is the first generation of its type (1). The format of the VOLSER is explained in 2.3.4, "Volume label format" on page 23.

Labelling service

This service applies only to the IBM 3589 model 002.

There are six characters in the VOLSER, and IBM provides specific codes to allow you the flexibility to choose where to begin the volume range you require. The sixth character is always zero as your volume serial range must always begin at a 0 boundary for labeling, and the labels supplied are sequential. So, for

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1375
3698
Doc

example, if you order 20 cartridges the first cartridge will be labeled with a sixth digit of 0, and the twentieth cartridge will be labelled with a sixth digit of 9.

The character identifier features are four-digit feature numbers of the form 9nnn, composed as follows:

- The first digit 9 means the feature carries no charge.
- A second digit of 1, 2, 3, 4, or 5 indicates which character in the VOLSER this feature is specifying (1st, 2nd, 3rd, 4th, or 5th).
- The third and fourth digits range from 00 through 35, where 00 through 09 represent the characters 1 through 9, and 10 through 35 represent the characters A through Z.

Choose the first 1, 2, 3, 4, or 5 digits by using the feature numbers as follows:

- First alphanumeric digit (0 to 9 or A to Z): use #9100 (0) to #9135 (Z).
- Second alphanumeric digit (0 to 9 or A to Z): use #9200 (0) to #9235 (Z).
- Third alphanumeric digit (0 to 9 or A to Z): #9300 (0) to #9335 (Z).
- Fourth numeric digit (0 to 9): use #9400 (0) to #9409 (9).
- Fifth numeric digit (0 to 9): use #9500 (0) to #9509 (9).
- Sixth numeric digit is set to 0 as standard.
- Seventh character of Volser is set to L.
- Eighth character of Volser is set to 1.

If you do not specify a feature number then the supplied starting character will be zero. Thus if you specify features for the first thee characters as ABC but no more, then the sequence of labels will begin ABC000.

Two specific features indicate requirements for colored labels:

- Feature #9077 specifies a white background.
- Feature #9022 specifies a colored background for the alpha characters.

If you specify #9022, then you can choose from 10 available colors shown in Table A-5 on page 231.

10523
A.

Table A-5 Color specify feature codes for the IBM 3589 model 002

Alpha prefix background	Feature code	Alpha prefix background	Feature code
red	9003	orange	9008
yellow	9004	pink	9009
light green	9005	dark green	9010
light blue	9006	light orange	9011
gray	9007	purple	9012

IBM media business distributors and other suppliers

If you want to buy additional supplies for the IBM LTO Ultrium product families you can obtain them from the IBM media business suppliers or third-party suppliers. To purchase in this way you must quote the Ultrium part numbers (not feature numbers or model types) for the different items required. The part numbers are listed in Table A-6.

Table A-6 LTO Ultrium 1 and 2 available supplies and part numbers

Part number	Description
08L9120	IBM LTO Ultrium 1 data cartridge
08L9870	IBM LTO Ultrium 2 data cartridge (no barcode label)
19P5887	IBM LTO Ultrium 2 data cartridge (with barcode label)
35L2086	IBM LTO Ultrium cleaning cartridge
08L9129	Leader pin attachment kit
08L9130	Cartridge rewind tool
13F5647	IBM tape unit cleaner
2108930	Lint-free cloth

To obtain these supplies or for warranty replacements, use the appropriate distributor for your country location:

- United States and Canada:
  For information about Priority Fulfillment Services distribution channels call 1-888-IBM-MEDIA in the U.S. and Canada.

RQS nº 03/2005 CN
CPMI - CORREIOS
Nº 1376
Doc 3698

- Latin America:
  For information about Priority Fulfillment Services distribution channels call +1-972-881-0733.
- Asia Pacific:
  For information about Priority Fulfillment Services distribution channels call +81-3-3808-8486 in Japan or +1-972-881-0733 outside of Japan.
- Europe, Middle-East, and Africa:
  For information about Priority Fulfillment Services Europe distribution channels call +31-433-502-756.
- Other country-specific numbers can be found at:

  `http://www.storage.ibm.com/media/lto/index.html`

Abbreviations and acronyms

AC	Alternating Current
AIM	Automatic Identification Manufacturers
AIT	Advanced Intelligent Tape
AIX	Advanced Interactive Executive
ALDC	Adaptive Lossless Data Compression
AME	Advanced Metal Evaporative
AMP	Advanced Metal Evaporative
ANSI	American National Standards Institute
API	Application Programming Interface
ATF	Auto Tracking Following
BRMS	Business Recovery and Management Services
CM	Cartridge Memory
CRC	Cyclic Redundancy Check
CVE	Compliance Verification Entity
DAT	Digital Audio Tape
DC	Direct Current
DDS	Digital Data Standard
DLT	Digital Linear Tape
ECC	Error checking and correction
ECMA	European Computer Manufacturer's Association
EEPROM	Electrically Erasable Programmable Read-Only Memory
EOT	End of tape
EOV	End of volume
ESCON	Enterprise Systems Connection
FC	Fibre channel/feature code
FC-AL	Fibre channel arbitrated loop
FCP	Fibre channel protocol
FICON	Fiber Connectivity
FRU	Field replacable unit
HBA	Host bus adapter
HSM	Hierarchical storage management
HVD	High voltage differential
IBM	International Business Machines
IDRC	Improved Data Recording Capability
IOP	Input/output processor
ISV	Industry solution provider
ITSO	International Technical Support Organization
LAN	Local area network

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1377
3698
Doc

LGMR	Laser Guided Magnetic Recording
LIP	Loop initialization protocol
LPAR	Logical partition
LPOS	Longitudinal Positioning
LTO	Linear Tape Open
LTO-CM	Linear Tape Open-cartridge memory
LTO-DC	Linear Tape Open Data Cartridge
LUN	Logical unit number
LVD	Low voltage differential
MCC	Medium changer controller
MES	Machine equipment specification
MFM	Modified Frequency Modulation
MIB	Management information block
MRC	Magneto-Resistive Cluster
MTBF	Mean time between failures
OEM	Original equipment manufacture
P/N	Part number
PCBA	Printed circuit board assembly
PCI	PC Connect interface
POS	Pivoting Optical Servo
PRML	Partial Response Maximum Likelihood
PTF	Program temporary fix
QIC	Quarter inch cartridge
RF	Radio frequency
RLL	Run Length Limited
RMU	Remote Management Unit
SAN	Storage Area Network
SARS	Statistical Analysis and Reporting System
SCSI	Small computer systems interface
SDG	SAN Data Gateway
SDLT	SuperDLT
SLDC	Streaming lossless data compression
SMIT	Systems Management Interface Tool
SNIA	Storage Networking Industry Association
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
VHDCI	Very High Density Cable Interconnect
VPD	Vital Product Data
WWN	World Wide Name

10519
A.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see "How to get IBM Redbooks" on page 237. Note that some of the documents referenced here may be available in softcopy only.

- *Storage Area Networks: Tape Future in Fabrics*, SG24-5474
- *Designing an IBM Storage Area Network*, SG24-5758
- *Using IBM LTO Ultrium with Open Systems, SG24-6502*
- *Implementing IBM LTO in Linux and Windows*, SG24-6268
- *IBM Tivoli Storage Manager Version 5.1 Technical Guide*, SG24-6554

Other publications

These publications are also relevant as further information sources:

- *IBM TotalStorage Tape Device Drivers Installation and User's Guide*, GC35-0154
- *IBM TotalStorage Tape Device Drivers Programming Reference*, GC35-0346
- *IBM Ultrium Device Drivers Installation and User's Guide*, GA32-0430
- *IBM 3580 Ultrium Tape Drive Setup, Operator, and Service Guide*, GA32-0415
- *IBM 3581 Ultrium Tape Autoloader Setup, Operator, and Service Guide*, GA32-0412
- *IBM 3582 Ultrium Tape Library Setup, Operator, and Service Guide*, GA32-0548
- *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411
- *IBM 3584 UltraScalable Tape Library Planning and Operator Guide*, GA32-0408

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1378
3698
Doc

Online resources

These Web sites and URLs are also relevant as further information sources:

- This is the main Web site for information about IBM LTO products:

  `http://www.ibm.com/storage/lto`

- The Linear Tape Open Technology Organization Web site provides information about the technology, formats and licensing:

  `http://www.lto-technology.com/`

- The SCSI Trade Association Web site provides information about SCSI standards and terms:

  `http://www.scsita.org`

- This Web site describes the media available from IBM:

  `http://www.ibm.com/storage/media`

- This Web site describes IBM Microelectronics products including compression devices:

  `http://www.chips.ibm.com`

- This Web site describes the Streaming Lossless Compression Algorithm:

  `http://www.ecma-international.org/publications/standards/ECMA-321.HTM`

- IBM Tivoli Storage Manager SAN device support:

  `http://www-3.ibm.com/software/tivoli/products/storage-mgr-san/platforms.html`

- Ultrium device driver downloads:

  `ftp://ftp.software.ibm.com/storage/devdrvr`

- LTO devices update drive firmware:

  `http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_drivefw`

- ISV Support Matrix for LTO:

  `http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

- Ultrium 3580 Drive firmware information:

  `http://www-1.ibm.com/support/docview.wss?rs=543&org=ssg&doc=S4000055&loc=en-us`

- IBM 3582 Interoperability Matrix:

  `http://www.storage.ibm.com/tape/lto/3582/3582opn.pdf`

- IBM 3583 Interoperability Matrix:

  `http://www.storage.ibm.com/tape/lto/3583/3583opn.pdf`

10517
A.

- IBM 3584 Interoperability Matrix:

  `http://www.storage.ibm.com/tape/lto/3584/3584opn.pdf`
- IBM 3584 drive and library firmware:

  `ftp://ftp.software.ibm.com/storage/358x/3584`
- IBM HBA and SAN Interoperability Matrix:

  `http://ssddom02.storage.ibm.com/hba/hba_support.pdf`
- IBM Sales Manual:

  `http://www.ibmlink.ibm.com/ussman`
- IBM ServerProven compatibility for hardware, applications, and middleware:

  `http://www.pc.ibm.com/us/compat`
- IBM xSeries tape storage:

  `http://www.pc.ibm.com/ww/eserver/xseries/tape.html`
- IBM iSeries technical support:

  `https://techsupport.services.ibm.com/server/support?view=iSeries`

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1379
Doc: 3698

10516
A.

Index

Numerics

3580 see IBM 3580
3581 see IBM 3581
3582 see IBM 3582
3583 see IBM 3583
3584 see IBM 3584
8 mm tape 56
9210 121
9211 122
9212 122
9400 122
9600 122

A

activity status display 197
Advanced Metal Evaporative media 51
AIT 57
AIX commands
  cfgmgr 176
ALDC 16–17
arbitrated loop 33
archive life 25
Atape driver 176
autoloader 67
automated tape libraries 68
availability features 41

B

backup 17
bands 6, 10
bands See also servo tracks
barcode
  format 22
barcode label 19
barcode label format 22
barcode reader 117, 132, 202
brick 28

C

call-home 179
capacity 18
capacity, calculation for IBM 3584 185
cartridge door 19
cartridge handling 25
cartridge inspection 27
cartridge life 24
cartridge memory 7, 20, 42
cartridge shipping 26
cartridge slot columns 181
cfgmgr 176
channel calibration 38
cleaning 43, 90, 111, 210
  IBM 3580 91
  IBM 3582 128
  IBM 3583 156
cleaning cartridge 25, 43
codewords 17
coercivity 20
common subassembly 28
compression 16
compression scheme swapping 30
control path 46
control path failover 47, 175

D

DAT 54
data bands 6, 13
data compression 16, 30
data rate 28, 50
  burst 35–36
data tracks
  number of 16
DDS 54
diagnostic cartridge 182
differential SCSI 32
Digital Audio Tape 54
Digital Data Standard 54
Digital Linear Tape 58
direction buffer 16
disaster recovery 74
DLT 58
DLT 2000 60
DLT 4000 60
DLT 7000 61
DLT 8000 61

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1380
Doc. 3698

dual-gripper 174
dynamic speed matching 37

E
EEPROM 20
element addresses 194, 196
element numbers 105, 194
enterprise tape libraries 68
error correction 7, 41

F
fast locate function 21
FCA 169, 175, 191
FC-AL 33
Feature
  1603 188
  7003 100
  7004 100
  8001 225
  8002 225
  8003 132, 137
  8004 132, 137
  8006 142
  8008 142
  8012 141
  8105 132
  9022 230
  9077 230
  9210 143, 192
  9211 143, 192
  9212 143, 192
  9213 143, 192
  9215 143
  9400 143, 192
  9600 143, 192
Fibre channel 33
  native 33
firmware 112, 179
  IBM 3580 91
flat lap head 42
frame controller assembly see FCA

G
grips 19

H
HD68 34
helical-scan recording 50
HVD 80, 95, 115, 132

I
I/O station 185
IBM 113
IBM 3480 63
IBM 3490E 63
IBM 3494 161
IBM 3580 45, 79
  application software support 86
  cartridges 87, 123, 206
  device driver 84–85
  display 89
  feature codes summary 81
  firmware 91
  implementation 87
  interposer 83
  L11 80
  media 87
  Model H11 80
  Model H23 80
  Model L11 80
  operating modes 110
  SCSI adapters 82
  SCSI cables 82
  SCSI ID 87
  SCSI length limitations 83
  server attachments 84
  status light 88
  Storage Applications 86
  unload 90
  upgrade 84
  warranty 81
IBM 3581 45, 93
  access mode 96
  activity bar 107
  barcode reader 98
  cartridge I/O 97
  cleaning 111
  control buttons 108
  device driver 102
  drive status 107
  error code 107
  feature codes summary 96
  general information 95
  Initial setup 104
  interposer 99

library modes 96, 110
media 87, 103
media cartridges 103
message display panel 106
Model H17 95
Model L17 95
operator display 105
optional bar code reader 100
performance considerations 86, 103
SCSI adapter 98
SCSI cables 98
SCSI devices 97
setting SCSI addresses 104
status light 105
storage applications 103
warranty 96
IBM 3582 45, 113
application software support 123
barcode reader 117
capacity 114
cleaning 128
device driver 122
element addresses 125
feature codes summary 118
firmware 128
general information 114
I/O station 117
implementation 124
interposer 121, 140
inventory 117
inventory update 117
library control unit 117
library modes 128
magazines 115
maintenance 118
media 87, 123
model description 114
multi-path architecture 114, 124
operator panel 118, 125–126
performance considerations 124
robotic system 117
SCSI cabling 120
SCSI defaults 125
storage slots 115
IBM 3583 45, 129
cabling options 138
capacity 130
cartridge magazines 133
cleaning 156
control path 135
device driver 144
drive status 152, 209
element addresses 150
feature codes summary 136
firmware 157
general information 130
I/O station 133, 141
implementation 146
inventory 132–133
inventory update 132
library control unit 133
library mode 156
library status 151
magazines 132
maintenance 135
media 87, 145
menu options 127, 153
message display 151
Model L18 131
Model L36 131
Model L72 131
operator panel 134, 151
performance considerations 145
physical library layout 147
redundant power 142
Remote Management Unit 151, 154
RMU 151, 154
robotic system 133
SAN Data Gateway 135
SCSI adapters 137
SCSI defaults 147
SCSI ID and LUN assignment 146
SDG 135
storage columns 132
upgrade 131, 141
IBM 3584 45, 159
accessor 172
bandwidth 187
barcode reader 162, 174
bulk-loading 162
calibration sensor 174
call-home 179
capacity 160, 181
capacity calculation 185
Capacity Expansion feature 162
cartridge gripper 173
cartridge slots 163, 181
components 165

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1381
Doc. 3698

configuration 180
control path 194
control path failover 175
D32 frame 183
device drivers 192
diagnostic cartridge 182
distributed control system 167, 170
drive features 166
Dual AC Power 191
dual-gripper 174
element addresses 194, 196
element numbers 194
expansion frame 161, 188, 196
features 188
firmware 179
floor requirements 190
Frame Control Assembly Feature 163
general information 160
I/O station 162, 177, 185
implementation 194
inventory 186
inventory time 188
library control system 167
logical address 196
LTO Ultrium drives 166
major components 165
media 87
mode of operation 198
Model D32 161, 163, 188
Model L32 161, 181
multi-path architecture 134, 194
operating environment 191
operator display 196
operator panel 171
performance 186
physical address 196
physical dimensions 189
pivot assembly 173
power and cooling 191
rail assembly 174
reliability 177
remote support 179
Remote Support Attachment 179
Remote Support Switch 179
SNMP see SNMP
StorWatch Specialist 176
tape drive element numbers 195
tape drives 162
upgrade options 188
upgrades 188
Vital Library Data 178
Vital Product Data 198
WWN 174
IBM 3607-26X 199
barcode reader 202
capacity 200
element addresses 207
feature codes 205
firmware 210
general information 200
I/O station 202
inventory 202
library manuals 211
library mode 210
media 206
menu options 210
operator panel 208
physical dimensions 206
IBM 4560-SLX 199, 208
barcode reader 202
capacity 201
element addresses 207
Elevator Link Extension Option 201
Elevator Link Option 201
feature codes summary 204
firmware 210
general information 201
I/O station 202
inventory 202
library manuals 211
library mode 210
media 206
menu options 210
operator panel 208
physical dimensions 206
IBM Magstar 3590 64
IBM TotalStorage Enterprise Automated Library 3494 161
IBM TotalStorage UltraScalable Tape Library 3584 see IBM 3584
IBM TotalStorage Ultrium Tape Autoloader 3581 see IBM 3581
IBM TotalStorage Ultrium Tape Drive 3580 see IBM 3580
IBM TotalStorage Ultrium Tape Library 3582 see IBM 3582
IBM TotalStorage Ultrium Tape Library 3582 see IBM 3582

implementation 104, 124, 207
IBM 3580 87
input/output station 162, 177
integrated cleaning mechanism 90
interchangeability of drives 45
interfaces 31
interleaved recording 10
inventory 117, 132, 202

L
label area 19
labelling 229
leader pin 19
library centric WWN 175
Library Control Unit 203
library partitioning 47
library sharing 46, 134
library upgrade 45
linear recording 6, 50
Linear Tape Open
see LTO
load-to-ready time 35–36
locking mechanism 19
logical library 134
longitudinal positioning 12
LPOS 13
LTO 1
barcode 22
cartridge life 24
cartridge memory 20
cleaning cartridge 25
data compression 30
formats 2
interfaces 31
inter-generation compatibility 39
license packages 4
licensing 3
media identifier 23
power supply 28
reliability and availability 41
shelf life 21
specifications 3
LTO 2
performance 36
LTO-CM 20, 24
data fields 21
LTO-DC 16
LVD 80, 95, 115, 132

M
magazine numbering 148
magazines 132–133
Magstar 64
maintenance 204
Mammoth 57
Management Information Base see MIB
MCP
media 223, 225
suppliers 231
media compatibility 20
media labelling 229
Media sharing 72
medium changer pack see MCP
metal particle media 20, 51
MIB 180
multi-path architecture 46, 114, 124, 134, 194
multiple filemarks 38

N
NetView 180
notches 19

O
offsite vaulting 74
operating modes 110
operator interface 170
operator panel 118, 134, 204, 208

P
Partial Response Maximum Likelihood 36
PAUSE 197
performance
load-to-ready 35–36
search time 35–36
unload time 35–36
physical address 195
Pivoting Optical Servo 62
POST 179
power management 38
Power On Self Test see POST
power supply 28

Q
QIC 52
QIC standards 54
quarter-inch cartridge 52

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1382
Doc. 3698

R

random access mode 110
RAS 41, 177
  IBM 3584 177
read/verify elements 16, 29
recording format 6
Redbooks Web site 237
  Contact us xxii
Remote Management Unit 134
remote support 179
Remote Support Attachment 179
Remote Support Switch 179
RMU 134
robotic control 203

S

SAN 68
  Loop 71
  Point-to-point 71
  Server to server 69
  Server to storage 69
  Storage to storage 69
  Switched 71
SAN topologies 71
SARS 21, 42
scheme swap 17
SCSI 31
  adapter 82
  address for autoloader 97
  autoloader address 125
  cabling 205
  element address 196
  element numbers 105
  HVD differential 32
  LVD differential 32
  single ended 32
SCSI ID 87
SDLT 62
search time 35–36
sequential access mode 110
serpentine linear recording 51
serpentine recording format 28
Server-free backup 76
servo
  timing based 7
servo bands 11
servo bursts 11
servo elements 30
servo tracks 10, 20, 51
shelf life 25
SNMP 180
  MIB 180
Sony AIT 57
speed matching 37
Statistical 42
Statistical Analysis and Reporting System
  see SARS
status LED 39
STK 9840 65
StorWatch 176
SuperDLT 62
Surface Control Guiding 41
switch
  electronic head switch 29
switch fabric connection 33

T

tape drive assembly 166
tape format specifications 5
tape head cleaner 41
tape length 18
tape media
  coating 20
  material 20
threading mechanism 29
Track Following 11
tracks
  number of 6
  positioning 7
TSM
  Managed System for SAN 75

U

Ultrium
  capacity 6
  cleaning cartridge 43
  media 87
  media features 225
  recording format 6
Ultrium 1
  capacity 18
  interfaces 35
  number of tracks 6
  performance 35
  tape length 18
Ultrium 2

10510
A.

capacity 18
channel calibration 38
interfaces 35
media features 225
multiple filemarks 38
number of tracks 6
performance 36
power management 38
speed matching 37
tape length 18
Ultrium Cartridge 18
Ultrium drive 28
display 39
Ultrium tape 9
universal cleaning cartridge 25
unload time 35–36

V

VHDCI 34
volume label format 23
volume serial number 22

W

wrap 14, 30
write process 14
write protect switch 24

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1383
Doc. 3698

IBM

Redbooks

The IBM LTO Ultrium Tape Libraries Guide

(0.5" spine)
0.475"<->0.875"
250 <-> 459 pages

10509
VA.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1384
Doc. 3698

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1385
Doc 3698

10503
CA.

IBM®

The IBM LTO Ultrium Tape Libraries Guide

Redbooks

Understand Linear Tape-Open technology and its unique architecture

Learn about the IBM Ultrium drives and libraries

Updated for Ultrium LTO 2 products

This IBM Redbook presents a general introduction to Linear Tape-Open (LTO) technology and the implementation of corresponding IBM products. As such it describes both general LTO technology specifications and specific details of the unique design of IBM Ultrium tape drives and libraries.

In addition to the description of LTO, the reader will find technical information about each of the IBM Ultrium products, including generalized sections about SCSI and Fibre Channel connections, multi-path architecture configurations, and tape technology comparisons with market positioning.

This book is intended for anyone who would like to understand more about the general LTO technology specification and how it came about, as well as the IBM implementation of that specification.

The second edition of this book covers the second generation LTO products as well as the original LTO products.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-5946-01 ISBN 0738453226

10507
A.

Manual 7

2109 Model M12
User`s Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1386
Doc 3698

IBM TotalStorage SAN Switch

10506
CA

2109 Model M12 User's Guide

Read Before Using

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1387
3698
Doc.

GC26-7468-02

IBM TotalStorage SAN Switch

10505

2109 Model M12 User's Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
1388
Fls. Nº
Doc. 3698

GC26-7468-02

10504 A.

Note:
Before using this information and the product it supports, read the general information in "Safety and environmental notices" on page xi and "Notices" on page 51.

Third Edition (May 2003)

This edition replaces GC26-7493-01.

© Copyright International Business Machines Corporation 2002, 2003. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

10503
CA.

Contents

Figures vii

Tables ix

Safety and environmental notices xi
Safety label checks xi
Environmental notices and statements xiii
Laser safety xiii
Battery notice xiv
Fire suppression systems xiv
Product recycling xiv
Product disposal xiv

About this document xv
Who should read this document xv
Additional information xv
2109 Model C36 with Model M12 library xv
Related documents xv
Web sites xvi
Getting help xvi
Getting software updates xvi
How to send your comments xvii

Introduction 1
Product overview 1
Throughput 2
Link distance 2
SFP fiber optic transceivers 2
System design overview 3
High availability 4
Reliability 4
Serviceability 5
Ports 5
Numbering 6
Rack mounting 6
Cooling system 6
Cable management 7
Worldwide name LED card 7
Power distribution system 7
Power distribution strategy 8
ac input 8
dc outputs 8
2N power architecture 8
CP blade assembly 9
CPU subsystem 9
Configuration 10
Management 10
Switch blade assembly 11
Switch blade assembly design 11
Fault monitoring and diagnostics 12
Diagnostic tests 12
System status indicators 12
Software features 13

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1389
Doc. 3698

Fabric OS 14
Interoperability 15
Security 15
Network manageability 15
Field replaceable units (FRUs) 16

Appendix A. Product specifications 17
2109 Model M12 components 17
Physical dimensions 17
2109 Model M12 and component weights 17
2109 Model C36 with Model M12 specifications 18
16-port card specifications 18
CP card specifications 18
Facility specifications 20
Power specifications 21
Environmental requirements 22
General specifications 22
Regulatory specifications 23

Appendix B. Safety certifications and regulatory compliance 25
Safety 25
EMI/EMC 25
Immunity 26

Appendix C. Danger and caution notice translations 27
Arabic 27
Brazilian-Portuguese 28
Chinese, simplified 29
Chinese, traditional 30
Croatian 31
Czech 32
Danish 33
Finnish 34
French 35
German 36
Greek 37
Hebrew 38
Hungarian 40
Italian 41
Japanese 42
Korean 43
Macedonian 44
Portuguese 45
Russian 46
Slovak 47
Slovenian 48
Spanish 49
Swedish 50

Notices 51
Trademarks 52
Electronic emission statements 52
Federal Communications Commission (FCC) statement 52
Industry Canada compliance statement 52
Chinese Class A compliance statement 52
European Community compliance statement 53

10501
A

Germany compliance statement. 53
Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 54
Korean Government Ministry of Communication (MOC) statement 54
Taiwan class A compliance statement 54

Glossary 55

Index 69

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1390
3698
Doc.

10500
A.

Figures

1. Safety label on the 2109 Model M12 xii
2. Linecord caution label xii
3. SFP label (front view) xii
4. SFP label (back view) xiii
5. 2109 Model M12 (cable side and noncable side) 4

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1391
Doc. 3698

1049
A

Tables

1. Brocade and IBM product and model number matrix. xvi
2. Power distribution system specifications 7
3. Power supply configurations 9
4. Cable side LEDs 12
5. Noncable side LEDs 13
6. Physical dimensions of the 2109 Model M12 17
7. Component weights 17
8. 2109 Model C36 with Model M12 specifications 18
9. Memory specifications 19
10. Battery specifications 19
11. Terminal serial port pinouts 19
12. Modem serial port pinouts 20
13. Power specifications 21
14. Environmental requirements 22
15. General specifications 22
16. Regulatory specifications 23

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1392
Doc: 3698

Safety and environmental notices

Safety notices are printed throughout this document.

A *danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

A *caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

An *attention* notice indicates the possibility of damage to a program, device, system, or data.

For translations of danger notices and caution notices, see Appendix C, "Danger and caution notice translations", on page 27. The notices are listed in numeric order based on their IDs, which are displayed in parentheses at the end of each notice. See the following examples of danger notices and caution notices for the location of the ID numbers.

DANGER

To prevent possible electrical shock during an electrical storm, do not connect or disconnect cables or station protectors for communications lines, display stations, printers, or telephones. (1)

CAUTION:
A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery may present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations. (1)

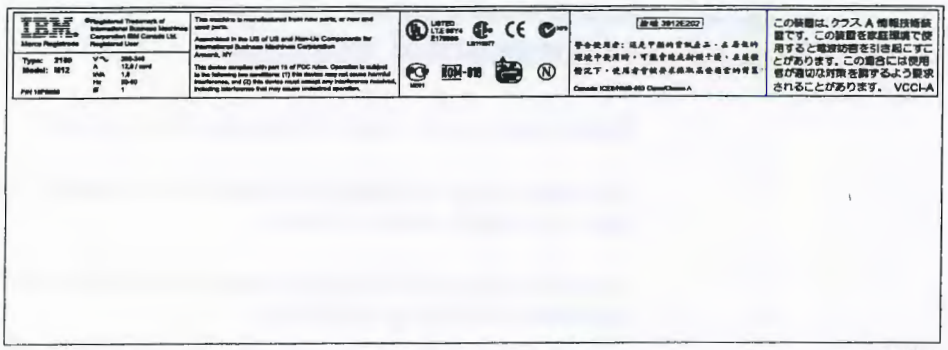
Safety label checks

Perform the following safety label checks:

1. Verify that the safety label shown in Figure 1 on page xii is installed on the 2109 Model M12.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 1393
Doc. 3698

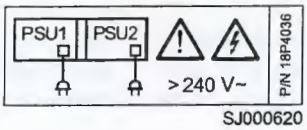


SJ000623

Figure 1. Safety label on the 2109 Model M12

2. Verify that the linecord safety label shown in Figure 2 is installed on the power supply of the 2109 Model M12.

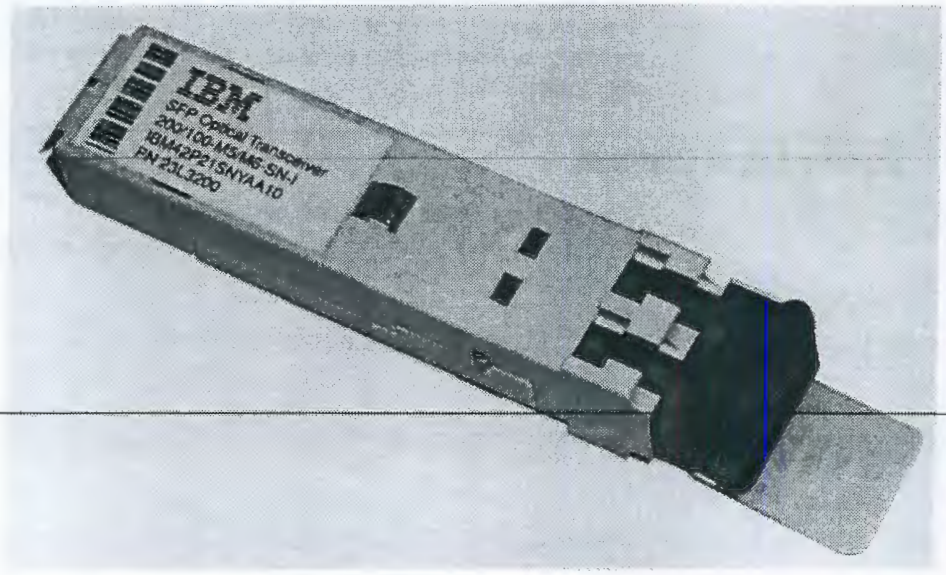
   CAUTION:
   This unit may have two linecords. To remove all power, disconnect both linecords. (1)



SJ000620

Figure 2. Linecord caution label

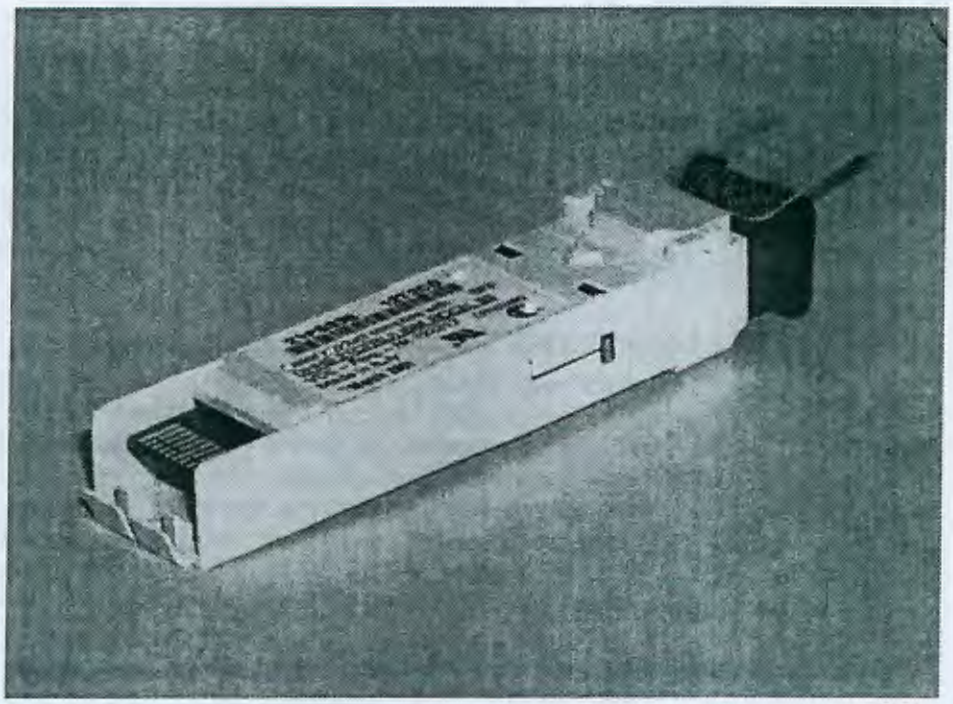
3. Verify that the SFP label shown in Figure 3 and Figure 4 on page xiii is installed on the 2109 Model M12.



SJ000317

Figure 3. SFP label (front view)

10495
CA.



SJ000314

Figure 4. SFP label (back view)

Environmental notices and statements

This section describes the environmental notices and statements.

Laser safety

CAUTION:
In the United States use only GBIC units or Fibre-Optic products that comply with FDA radiation performance standards, 21 CFR Subchapter J. Internationally use only GBIC units or Fibre-Optic products that comply with IEC standard 825-1. Optical products that do not comply with these standards may produce light that is hazardous to the eyes.

SJ000327

This unit might contain a single-mode or a multimode transceiver Class 1 laser product. The transceiver complies with IEC 825-1 and FDA 21 CFR 1040.10 and 1040.11. The transceiver must be operated under the recommended operating conditions.

This equipment contains Class 1 laser products, and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser safety standard IEC 825-2.

Usage restrictions

The optical ports of the modules must be terminated with an optical connector or with a dust plug.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1394
Doc. 3698

Battery notice

CAUTION:
A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery may present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations. (3)

Fire suppression systems

A fire suppression system is the responsibility of the customer. The customer's own insurance underwriter, local fire marshal, or a local building inspector, or both, should be consulted in selecting a fire suppression system that provides the correct level of coverage and protection. IBM designs and manufactures equipment to internal and external standards that require certain environments for reliable operation. Because IBM does not test any equipment for compatibility with fire suppression systems, IBM does not make compatibility claims of any kind nor does IBM provide recommendations on fire suppression systems.

Product recycling

This unit contains recyclable materials. These materials should be recycled where processing sites are available and according to local regulations. In some areas, IBM provides a product take-back program that ensures proper handling of the product. Contact your IBM representative for more information.

Product disposal

This unit might contain batteries. Remove and discard these batteries, or recycle them, according to local regulations.

10493
A.

About this document

This document introduces the IBM® TotalStorage™ SAN Switch 2109 Model M12 (hereafter referred to as the 2109 Model M12).

Who should read this document

This document is intended for network and system administrators whose responsibilities include administering and managing a storage area network (SAN).

Additional information

This section contains the following information:

- A list of the documents in the 2109 Model C36 with Model M12 library
- A list of the related documents
- The available Web sites
- Instructions on how to get help
- Instructions on how to get software updates
- Information about how to send your comments

2109 Model C36 with Model M12 library

The following documents contain information related to this product:

- *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*, GC26-7467
- *IBM TotalStorage SAN Switch 2109 Model M12 User's Guide*, GC26-7468 (this book)

Related documents

Information related to the 2109 Model M12 software can be found in the following documents:

- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Diagnostic and System Error Message Reference*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Reference*
- *Brocade Fabric Watch User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade MIB Reference*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Silkworm 12000 Core Migration User's Guide*
- *Building and Scaling Brocade SAN Fabrics: Design and Best Practices Guide*

When you use any of the Brocade documents, you will notice that the model numbers reflect the original Brocade switches. Table 1 on page xvi provides a product matrix for you to use to correlate the Brocade model numbers to the IBM

© Copyright IBM Corp. 2002, 2003

ECT n° 03/2005 - GN
CPMI - CORREIOS
Fls. Nº 1395
Doc 3698

product and model numbers.

Table 1. Brocade and IBM product and model number matrix

Brocade model number	IBM product and model number
Silkworm 2010	3534 Model 1RU
Silkworm 2400	2109 Model S08
Silkworm 2800	2109 Model S16
Silkworm 3200	3534 Model F08
Silkworm 3800	2109 Model F16
Silkworm 3900	2109 Model F32
Silkworm 12000	2109 Model M12

Web sites

For detailed information about models and firmware that the switch supports, see the following Web site:

www.ibm.com/storage/fcswitch/

For detailed information about Fibre Channel standards, see the Fibre Channel Association Web site at:

www.fibrechannel.com/

For a directory of worldwide contact information, including technical support, see the following Web site:

www.ibm.com/contact/

Getting help

Contact your switch supplier for technical support. This includes support of hardware, all product repairs, and ordering of spare components.

Be prepared to provide the following information to the support personnel:

- The switch serial number
- The switch worldwide name
- The topology configuration
- Any output from the **supportShow** Telnet command
- A detailed description of the problem
- Any troubleshooting steps that were already performed

Getting software updates

Contact your software vendor for software updates and maintenance releases.

For utility programs to facilitate loading firmware, sample Fabric Watch configurations, and management information base (MIB) files for switch management by simple network management protocol (SNMP), see the following Web site:

www.storage.ibm.com/ibmsan/products/sanfabric.htm

1049
A

How to send your comments

Your feedback is important to help us provide the highest quality of information. If you have any comments about this document, you can submit them in one of the following ways:

- E-mail

  Submit your comments electronically to:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the document and, if applicable, the specific location of the text that you are commenting on, such as a page number or table number.

- Mail or fax

  Fill out the Readers' Comments form (RCF) at the back of this document and return it by mail or fax (1-800-426-6209) or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Dept. M86/Bldg. 050-3
  5600 Cottle Road
  San Jose, CA 95193-0001
  U.S.A.

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 1396
Doc: 3698

10489
A-

Introduction

This chapter describes the TotalStorage SAN Switch 2109 Model M12, hereafter referred to as the 2109 Model M12. It provides the following information:

- "Product overview"
- "System design overview" on page 3
- "Power distribution system" on page 7
- "CP blade assembly" on page 9
- "Switch blade assembly" on page 11
- "Fault monitoring and diagnostics" on page 12
- "Software features" on page 13
- "Field replaceable units (FRUs)" on page 16

Product overview

The 2109 Model M12 represents the next generation of advanced Fibre Channel switches that are used to intelligently interconnect storage devices, hosts, and servers in a storage area network (SAN). It is a revolutionary product, a dual 64-port Fibre Channel switch that delivers unprecedented performance, scalability, flexibility, functionality, reliability, and availability.

- The 2109 Model M12 delivers a very high-density port, rack-ready solution to drive cost-effective SAN.
- The dual switch capability allows either one or two 64-port switches per chassis. You can interconnect the switches to create a high port count solution, or you can use them in a dual fabric, high availability topology.
- The 2109 Model M12 supports 1 Gbps and 2 Gbps auto-sensing Fibre Channel ports. Trunking technology groups up to four ports together to create high performance 8 Gbps inter-switch links (ISL) trunks between switches.
- Universal ports self-configure as expansion ports (E_ports), fabric ports (F_ports), or fabric loop ports (FL_ports).
- Small form-factor pluggable (SFP) optical transceivers support any combination of short wavelength (SWL) and long wavelength (LWL) optical media on a single switch module.
- The 2109 Model M12 offers a high availability platform for mission-critical SAN-designed applications.
- Dual redundant control processors (CPs) provide high availability and enable nondisruptive software upgrades.
- The 2109 Model M12 offers forward and backward compatibility with all 3534 and 2109 series switches.
- The Fabric operating system (OS) delivers distributed intelligence throughout the network and enables a wide range of value-added applications including Extended Fabrics, Fabric Access, Fabric Watch, Remote Switch, Web Tools, Secure Fabric OS, Advanced Zoning, and Advanced Security feature.
- High availability redundant design, extensive diagnostics, and system monitoring capabilities integrated with Fabric OS management tools deliver unprecedented reliability, availability, and serviceability.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1397
3698
Doc.

The 2109 Model M12 is a nonblocking core fabric switch. It never prevents a server from being able to connect to storage, even under congestion. The backplane bandwidth between ports on a 2109 Model M12 is sufficient to allow traffic to flow at full bandwidth.

Throughput

The 2109 Model M12 provides continuous and sustained bandwidth to all ports in a single or dual 32-port or 64-port switch scenario at their rated line speed. Throughput is 2.125 Gbps inbound and outbound per port. All ports can be simultaneously loaded for up to 100% utilization at full bandwidth. The backplane can handle future support for a 128-port switch, 10 bps Fibre Channel, IP connectivity, application processing and Infiniband.

Each port on the 2109 Model M12 is auto-sensing and supports 1 Gbps or 2 Gbps speeds. You can manually set the ports to support either 1 Gbps or 2 Gbps links. The ports perform speed-matching, which allows 1 Gbps and 2 Gbps links to mix on any route within the fabric. When there is 1 Gbps in and 2 Gbps out, the ASIC delays transmitting the outbound frame until half the frame is received at 1 Gbps. With 2 Gbps in and 1 Gbps out, the ASIC delays releasing the buffer to ensure that the 1 Gbps transmit port has adequate time to empty it.

Link distance

The 2109 Model M12 operates at up to 10 km (6.21 mi) at both 1 Gbps and 2 Gbps speed settings and supports LWL SFPs and single-mode fiber.

By using the Extended Fabrics optional software feature, the switch operates at distances greater than 10 km (6.21 mi) by using various methods. The switch leverages the current dense wavelength division multiplexing (DWDM) certification and is certified to interoperate with equipment from Optical Networks, Cisco Systems, Inc., Nortel Networks, and other leading vendors.

The switch operates at near full link speed at distances up to 100 km (62.13 mi) for 1 Gbps or 50 km (31.06 mi) for 2 Gbps speeds using the Extended Fabrics feature.

For information about Extended Fabrics, see the *Brocade Distributed Fabric User's Guide*.

SFP fiber optic transceivers

Each blade assembly supports up to 16 SFP fiber optic transceivers that convert electrical signals to optical signals (and optical signals to electrical signals) and are capable of transmitting at both 1 Gbps and 2 Gbps speeds.

Each SFP fiber optic transceiver supports 850 nm SWL, on multimode fiber optic cable, or 1310 nm LWL, on single mode fiber optic cable. These miniature optical transceivers meet the high port density that is available in the 2109 Model M12, deliver twice the port density of standard removable gigabit interface converter (GBIC) transceivers, and are encased in metal or shielded plastic to ensure low emissions and high thermal management. SFP devices are hot-swappable and connections are through industry-standard LC connectors.

104
A

System design overview

The 2109 Model M12 is highly available, modular, and scalable. High availability features include:

- Redundant CPs and CP hot-swappable replacements
- Dual redundant ac input and hot-swappable power supplies in the redundant power subsystem
- Hot-swappable blowers in the redundant cooling system
- Hot-swappable switch modules

The modular multi-blade assembly chassis of the 2109 Model M12 consists of:

- Up to eight hot-swappable 16-port switch blade assemblies that deliver up to two separate 64-port Fibre Channel switches in a single chassis. Each 64-port switch uses four blade assemblies.
- Two slots for CP blade assemblies

  A single active CP can control both logical switches in the chassis.
- Modular hot-swappable field replaceable units (FRUs):
  - Switch blade assembly
  - CP blade assembly
  - SFP optical transceivers
  - Blower assembly
  - Power supply
- Cables, blade assemblies, and power supplies that are serviced from the cable side of the switch, and blowers that are serviced from the noncable side. See Figure 5 on page 4, which illustrates the cable side and noncable side of the switch.
- A cable management tray and cable pillars
- Three blowers that provide cooling for the switch. The switch continues to operate indefinitely even if one blower fails.
- A worldwide name (WWN) light-emitting diode (LED) card on the noncable side that maintains chassis-specific information, such as WWNs, Internet Protocol (IP) addresses and summary status information of each blade assembly and power supply

ROS nº 03/2005 - CN
CPMI
Els Nº 1398
Doc. 3698

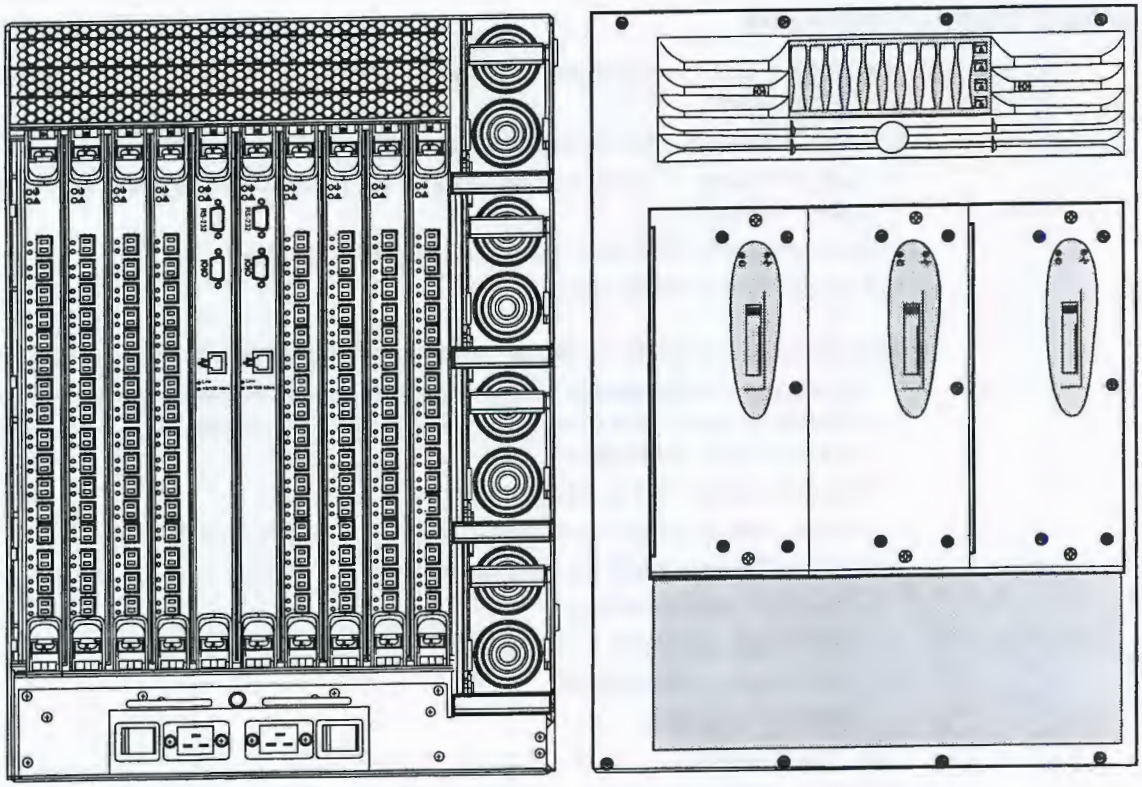


Figure 5. 2109 Model M12 (cable side and noncable side)

High availability

If a system is available, it is accessible 7 days a week and 24 hours per day. Availability is designated in terms of 9s. For example, the architecture of the 2109 Model M12 is designed for availability in excess of 99.999%.

The high availability software architecture of the 2109 Model M12 provides a common framework for all applications that reside on the system. High availability allows global and local states to be maintained so that any component failure is fully manageable.

Reliability

In addition to being available, the system must be reliable. This means that some, if not all, of its state must be maintained. In a reliable system, you are not aware of the internal state of a switch, and you experience continued system service with zero degradation.

The 2109 Model M12 provides the following features to ensure reliability:

- An error detection and correction mechanism to protect all data in the switch
- Power-on self test (POST)
- Error detection and fault isolation, such as cyclic redundancy checking (CRC), parity checking, checksum, and illegal address checking

1048
A-

- Dual CPs that enable hot, nondisruptive fast firmware upgrades. Each CP contains two serial ports and one Ethernet port. Offline CP diagnostics and remote diagnostics make troubleshooting easy. The Standby CP continuously runs diagnostics to ensure that it is operational should a failover be necessary.
- Inter-IC (I^2C) monitoring and control

For information about diagnostics, see the *Brocade Diagnostic and System Error Message Reference.*

Serviceability

The 2109 Model M12 provides the following features to enhance and ensure serviceability:

- Modular design with hot-swappable components
- Redundant flash memory that stores two firmware images per CP
- Extensive diagnostics and status reporting, along with a serial port to support an external, country-specific modem for remote diagnostics and status monitoring
- Nonvolatile random-access memory (NVRAM) that contains the OEM serial number, IBM serial number, revision information, and part number information
- Background health check daemon
- Memory scrubber, self test, and bus ping to determine if a bus is not functioning
- Watchdog timers
- Status LEDs
- Predictive diagnostics analysis through Fabric Watch
- SNMP integration with higher layer managers

For information about diagnostics, see the *Brocade Diagnostic and System Error Message Reference.* For information about Fabric Watch, see the *Brocade Fabric Watch User's Guide.*

Ports

Each switch blade assembly houses 16 auto-sensing 1 Gbps or 2 Gbps Fibre Channel ports and uses SFP optical transceivers.

The 2109 Model M12 supports the following port types:

- Optical ports
- Ethernet port
- Serial port

Optical ports

Fibre Channel interfaces of the 2109 Model M12 are equipped with an optical port interface that uses an SWL, 780 to 850 nm, or an LWL, 1270 to 1350 nm, laser transmitter. The laser complies with FDA21 CFR (J) Class 1 laser safety requirements. It uses non-Open Fibre Control (OFC) optical SFPs in the 2109 Model M12 series circuit. Safe Class 1 operation is guaranteed by limiting the optical power that is emitted by the port, which eliminates the need for physical shutters.

The optical SFP uses the LC-duplex connector scheme.

Ethernet ports

The 2109 Model M12 provides a fully IEEE compliant 10BASE-T or 100BASE-T Ethernet port for switch management. The port has two LEDs that indicates:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1399
Nº 3698
Doc.

- Speed (10 Mbps or 100 Mbps)
- Status of the connection

Additionally, each CP has its own Ethernet port. You can choose to connect the Ethernet ports to each other through an Ethernet switch or to connect them to separate networks for greater availability. Each CP has its own unique IP address and is accessible independent of the other CP.

Serial ports

Each CP comes with two serial ports. The top serial port on the installed CP is an RS-232 port that is used for remote dial-in. The bottom port is used for accessing the console.

Numbering

The 2109 Model M12 employs a numbering scheme that progresses from left to right and bottom to top in numerical order. The reference location is from the cable side of the chassis.

- Blade assemblies are numbered from 1 - 10, from left to right.
- Ports are numbered from 0 - 15, from bottom to top.
- Power supplies are numbered from 1 - 4, from bottom to top.
- Blowers are numbered from 1 - 3, from left to right.

Rack mounting

The mechanical design of the 2109 Model M12 allows rack mounting with either the cable side or the noncable side facing the front of the equipment rack. The chassis fits into a standard 19-inch EIA rack. Each chassis measures:

- 43.74 cm (17.22 in.) wide
- 70.87 cm (27.9 in.) deep (without the door)
- 61.24 cm (24.11 in.) high (less than 14U)

Cooling system

The 2109 Model M12 uses a redundant system of three hot-swappable blowers. Cool air intake is from the noncable side of the chassis, is pressurized, and is forced through the system. Heated air exits at the top of the cable side of the chassis. Three blowers that are used in conjunction with a pressurized plenum cool the unit. Each blower assembly includes a blower control assembly, which provides the following features:

- Blower status LEDs
- Blower speed sensing
- Blower speed control
- Serial electronically erasable programmable read only memory (EEPROM) that contains the part number, revision level, and error logs for the blade assembly
- Inlet air temperature monitoring

The 2109 Model M12 operates indefinitely if a single blower fails. When a blower assembly is removed, a mechanical flap seals the air chamber to maintain positive cooling air pressure in the chassis while the failed blower assembly is being replaced.

Cable management

10483
A

The cable management tray and cable pillars provide easy access to the 2109 Model M12 cables and allow you to organize and maintain the cables easily. Up to 128 pairs of fibre optic cables can be maintained on a single chassis. The cable management system is designed to allow any switch module to be replaced without disrupting service on any adjacent blade assemblies.

Worldwide name LED card

The WWN LED card is the neutral location to accommodate the worldwide unique serial ID for each logical switch on the 2109 Model M12. It is an integral part of the chassis. The serial EEPROM device contains multiple serial numbers for identifying the chassis, back plane, and the WWN card itself.

As an alternative system status indicator, this card consolidates the status of all modular components in the system on the cable side and presents the status to you in the form of LEDs on the noncable side. The arrangement of the LEDs on this card resembles the look of status LEDs on the other side of the switch.

The LEDs provide the summary of cable-side system status on the switch as follows:

- Two LEDs per blade assembly on the cable side of the cabinet
  - Green indicates that the power is OK.
  - Amber indicates that the blade needs attention.
- Two LEDs per power supply. Both LEDs are in the same location.
  - Green indicates that the power is OK.
  - Amber indicates that the power supply needs attention.

Power distribution system

The power subsystem is a redundant +48 V dc power distribution system with a provision for up to four 1000-watt, 48 V dc bulk power supplies. Bulk power supplies produce the intermediate distribution voltage in the distributed power system. See Table 2 for the power distribution system specifications.

Table 2. Power distribution system specifications

Specification	Value
Input voltage	A fully loaded switch requires a maximum of 2200 Volt-Amps. This results in a mains current of 9 amps at 240 V ac line voltage or 10 amps at 208 V ac line voltage. The rated ac input range is 180 - 264 V ac.
Supported power range	Nominal: 200 - 240 V ac, single phase
Input frequency range	47 - 63 Hz
Power supplies (each)	Output voltages: 48 V at 20 amps; 12 V at 4 amps Maximum output power: 1000 watts
ac inrush current	40 amps maximum, peak
Ride through	The power supply outputs remain within specified regulation for a minimum of 20 msec after the ac mains are disconnected.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1400
Doc: 3698

Table 2. Power distribution system specifications (continued)

Specification	Value
Under voltage protection	The 2109 Model M12 power supply self-protects from any input voltage, static or dynamic, from zero volts to its operating ranges. It recovers to normal operation when it returns to its operating range.

Power distribution strategy

All power for the blades comes from a single 48 V intermediate power bus. Great care is taken at each load to assure the integrity of the power bus.

The power supplies also provide a separate 12 V AUX voltage. This is used throughout the system to power the I²C logic and to monitor and control different system states.

ac input

Each ac input has an on-off circuit breaker switch. The power supply modules include input power filtering and power indicator LEDs. The power supply output remains within specific regulation for a minimum of 20 msec after the ac mains have been disconnected.

Two detachable line cords provide ac input power to the chassis.

dc outputs

The 2109 Model M12 uses up to four power supplies. All power supplies are hot-swappable. Two power supplies receive input power from one of the ac inputs. The remaining two power supplies receive power from the other ac input. Only two power supplies are required to run a completely loaded chassis. Therefore, if one ac input fails, and all power supply modules are populated, the chassis continues to run uninterrupted. If a power supply module fails, the remaining power supply modules continue to provide uninterrupted power to the chassis. The power supplies are plugged directly into their power bays to an internal blind connector.

Each blade assembly has separate dc-dc converter bricks for each voltage that is required. This allows local regulation at the blade assembly, and provides for future flexibility to match voltage needs with blade assembly type.

To maximize system availability when the switch blade assembly is plugged, it is initially powered off by the hardware. This ensures that adding a blade assembly does not bring the whole switch down if inadequate power is available. The system confirms sufficient power for the new module and then applies power. If sufficient power is not available (for example, if only one of the possible four power supplies are installed), the system does not allow more than four switch blade assemblies plus two CP blades to be powered up.

2N power architecture

The 2N power architecture is designed to protect against the loss of ac power. The 2109 Model M12 offers four power supply modules to assure maximum availability. Under normal operating conditions, only two power supplies are needed for full system operation. However, to ensure redundancy, two additional power supplies are available and are added in pairs, one per ac source.

Table 3 shows various supported power supply configurations and their respective levels of redundancy.

Table 3. Power supply configurations

Number of power supplies	Number of power cords	Number of switch blades	Number of CP blades	Number of blowers	Redundancy
1	1	4	2	3	No
2	1	4 or 8	2	3	Partial (See note)
3	2	4	2	3	Yes
4	2	8	2	3	Yes
Note: A single power cord results in the lack of ac source redundancy.					

CP blade assembly

The CP blade assembly controls the following 2109 Model M12 functions or features:

- System initialization
- Switch drivers
- High availability drivers
- Name server
- System management
- Fabric OS
- Fabric Manager
- Extended Fabrics
- Fabric Watch
- Remote Switch
- Web Tools
- Zoning

The CP blade assembly is compliant with the PCI Local Bus Specification 2.1. It provides all control and management functions in a 2109 Model M12 platform.

For more information about these features, see the following documents:

- *Brocade Fabric Watch User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Reference*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Advanced Zoning User's Guide*

CPU subsystem

The PowerPC 405GP 200-MHz microprocessor (PPC405) resides on the CP blade assembly. It contains a high-performance reduced instruction set computer (RISC) core, synchronous dynamic random access memory (SDRAM) controller, PCI bus

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1401
Doc. 3698

interface, direct memory access (DMA) engine, serial ports, I²C interface, read-only memory, and general purpose I/O. In addition, the CP blade assembly has the following functions:

- SDRAM controller that is built into the PPC405 with error correction support at 100 MHz
- SDRAM that supports 128 Mb configuration
- Socket PLCC32 boot flash that supports 512 Kb
- On-board compact flash that supports 256 Mb of software storage
- Two 32-bit, 33 MHz PCI-PCI bridges nontransparent
- Hot-plugged interface circuitry to support reliability, availability, serviceability and failover. If one device stops functioning, the other device automatically takes its place.
- One 10 Mbps or 100 Mbps management connection (RJ-45 connector type)
- Two universal asynchronous receiver-transmitter (UART) serial ports: one modem port for remote diagnostic testing and one terminal port for Telnet and command line interface (CLI) communication
- One amber LED to indicate the status for CP errors
- One green LED to indicate the proper operation for the CP power
- One green LED to indicate the system Ethernet 10 Mbps or 100 Mbps speed
- One amber LED to indicate the system Ethernet link status
- One digital thermometer for temperature sensing
- One real-time clock (RTC) with battery
- Two I²C I/O expander devices

Configuration

The CP blade assemblies can be configured to support a single 2-blade assembly topology, dual 2-blade assembly topology, a 4-blade assembly topology, a dual 4-blade assembly topology, or an 8-blade assembly switch topology. Other topologies can be supported on an as needed basis. Each CP interfaces to switch blade assemblies using a standard Peripheral Component Interconnect (PCI) bus. This bus runs at 33 MHz and can be 32 or 64 bits wide (bus 1 and 2). The CP blade assembly supports the following switch configurations:

- Single 32-port switch with dual CPs
- Dual 32-port switches with dual CPs
- Single 64-port switch with dual CPs
- Dual 64-port switches with dual CPs

Management

The CPs manage as many as eight switch blade assemblies within a single switch and monitor up to four power supplies, three blowers, three inlets (in the blower), up to 12 outlet temperature monitors (one per blade assembly), and other blade assembly-specific environmental features, such as voltages. The CP can individually reset each blade assembly, detect the status of each blade assembly (installed/not installed), manage the interrupt and service demand from each blade assembly, control the ability of a blade assembly to drive or not drive the PCI bus, and determine the error status of each blade assembly.

10479
A

Switch blade assembly

The switch blade assembly is a blade in the chassis of the 2109 Model M12. Each switch blade assembly provides 16 external Fibre Channel ports that run at 1 Gbps and 2 Gbps. A full switch consists of up to four switch blade assemblies and provides up to 64 ports in multiples of 16 ports.

The switch blade assembly is responsible for Fibre Channel switch circuitry and houses the switch application-specific integrated circuit (ASIC), backplane serial-deserializer (SERDES), external SERDES, and status LEDs for external SERDES such as port speed and port state, as well as the SFP fiber optic media. The SERDES performs two key functions. It receives the serial data stream of the system and converts it to a parallel stream. It also transmits parallel data streams to serial data streams.

Each switch blade assembly is hot-swappable and can be installed while the switch is running. Long pins, short pins, or both are used on the backplane to assure proper ground-voltage-signal sequencing. Field effect transistor (FET) switches, such as QuickSwitches, are used to isolate the PCI interfaces.

When a switch blade assembly is inserted, the power regulation circuitry inhibits the on-board dc converter (DCC) and maintains the switch blade assembly as turned off. The CP, under software control, enables the DCC and thus turns on the switch blade assembly. When the switch blade assembly is ready it interrupts the CP for initialization.

Each switch blade assembly has an on-board serial EEPROM that is only accessible through the I²C bus interface. This serial EEPROM can be accessed by a CP to determine information, including:

- OEM serial number
- IBM serial number
- Manufacturing date
- Manufacturing location
- Part number
- Revision
- Error logs

Switch blade assembly design

The switch blade assembly has the following dimensions:

- 42.06 cm (16.56 in.) high
- 29.74 cm (11.71 in.) wide
- 3.58 cm (1.41 in.) deep

Each switch blade assembly is connected to the backplane through high performance connectors.

The switch blade assembly provides 16 external Fibre Channel ports. Each of the 16 ports per blade assembly are auto-sensing, speed matching at 1 Gbps and 2 Gbps, support trunking, and are universal (E_port, F_port, and FL_port). Port speed can be managed through the management interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1402
Doc. 3698

Fault monitoring and diagnostics

Fault monitoring, diagnostic tests, and system status indicators simplify switch management and ensure the availability of the 2109 Model M12.

Diagnostic tests

Diagnostic testing occurs in three areas: power-on self test (POST), switch level testing, and manufacturing tests.

- The POST tests are blade oriented and ensure that the switch is ready for use. Testing is performed on physical ports.
- Switch level tests are done at the user port level. The tests rely on the standard Fabric OS support to provide routing and port setup.
- Manufacturing support includes long duration testing.

System status indicators

LEDs on the noncable side of the switch summarize the system status of each switch blade assembly, each CP blade assembly, and each power supply module. The blowers, which are accessible on the noncable side, also have LEDs that indicate their status.

Cable-side LEDs

Table 4 describes the appearance of the LEDs on the cable side of the system:

Table 4. Cable side LEDs

LED location	Indication
System status panel	• Green indicates that the blade assembly has power. • Amber indicates that the blade assembly needs attention.
CP blade assembly	Contains two additional LEDs for its Ethernet ports • Green indicates link speed. – On indicates 100 Mbps operation. – Off indicates 10 Mbps operation. • Amber indicates link status – Solid on indicates a link is not good. – Flashing indicates a link is OK. – Off indicates that no link is detected.
Each port on a switch card	Contains two LEDs • Top LED: – Green indicates 2.125 Gbps. – Off indicates 1.0625 Gbps. • Bottom LED: – Green indicates the port is operational. – Amber indicates the port is off or disabled.

10477
A

Table 4. Cable side LEDs (continued)

LED location	Indication
Each power supply	Contains three LEDs • Green – Solid indicates that ac is applied and power outputs are OK. – Flashing indicates that only the auxiliary output is valid. • Amber center light is a predictive failure light. It indicates that a power supply might fail due to a poorly performing fan. A replacement should be scheduled soon. • Amber lower light is a fault light. It indicates that a power supply has failed and a replacement is necessary.

Noncable side LEDs

Table 5 describes the appearance of the LEDs on the noncable side of the system:

Table 5. Noncable side LEDs

LED location	Indication
Blower	• Green indicates that the blade assembly has power. • Amber indicates that the blade assembly needs attention.
Blower system status panel	• Green indicates that the blower assembly has power. • Amber indicates that the blower assembly needs attention.

Additional status reporting functions are provided by the Fabric Watch feature. For information about Fabric Watch, see the *Brocade Fabric Watch User's Guide*.

Software features

Fabric OS version 4.1 supports the 2109 Model M12. Fabric OS includes all the basic switch and fabric support software as well as optionally licensed software that is enabled by using license keys. Fabric OS is made up of two major software components: firmware that initializes and manages the switch hardware, and diagnostics.

Optionally licensed and separately priced features include:

- Extended Fabrics (Feature code 7603)

  Provides up to 100 km (62.14 mi.) of switched fabric connectivity at full bandwidth over long distances
- Remote Switch (Feature code 7602)

  Enables switches to interconnect over wide area network (WAN) using third-party gateway solutions that support FC over IP, FC over ATM, and FC over SONET
- Advanced Security (Feature code 7623)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1403
3698
Doc

Enables policy-based security mechanisms that are integrated within Fabric OS

The following licensed software provides a graphical user interface from a standard workstation:

- Fabric Manager 4.0 (Feature code 7203)

  Administers, configures, and maintains fabric switches and SANs with host-based software

The following licensed features are included with the 2109 Model M12:

- Performance Monitoring

  Comprehensive tool for monitoring the performance of network storage resources
- ISL Trunking

  Connects up to four ISLs between two switches through an expansion port (E_port) to merge logically into one link
- Fabric Watch

  Monitors mission-critical fabric parameters
- Advanced Zoning

  Segments a fabric into virtual private SANs
- Web Tools

  Administers, configures, and maintains fabric switches and SANs

Note: To activate these features, go to the following Web site:

www.ibm.com/storage/key/

See the following documents for more information about Fabric Watch, Fabric Manager, Web Tools, Secure Fabric OS, and high availability:

- *Brocade Fabric Watch User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Fabric OS Reference*
- *Brocade Silkworm 12000 Hardware Reference Manual*

Fabric OS

Fabric OS is a robust operating system for high-performance, scalable SANs. Fabric OS allows you to:

- Rapidly build highly resilient, fault-tolerant multiswitch SAN fabrics
- Ensure high-speed access to business-critical data
- Allow hosts to dynamically share storage resources
- Rapidly scale the SAN by simply plugging in new devices with no configuration required. Software upgrades are nondisruptive
- Integrate private loops, private hosts, load balancing and sophisticated SAN management
- Easily manage the switches, hosts and devices that comprise the SAN

10474
A.

The Fabric OS for the 2109 Model M12 allows any Fibre Channel-compliant device to attach to the switches as long as it conforms to the device login, name service, and related Fibre Channel feature standards. Each operating environment requires that a Fibre Channel host bus adapter (HBA) be available with a standards-compliant driver for proper interface to the fabric.

Fabric OS consists of a set of embedded applications that run on top of an embedded real-time Linux operating system kernel. These applications include the following:

- Name server
- Alias server
- Simple Network Management Protocol (SNMP) agent
- Several tasks to manage the following:
  - Address assignment
  - Routing
  - Link initialization
  - Fabric initialization
  - Link shutdown
  - Switch shutdown
  - User interface

Interoperability

Fabric OS Version 4.1 interoperates with 3534 Model 1RU (minimum version 2.6). McData ED-5000 (from operating system version 4.0) interoperability is also provided.

Security

Secure Telnet access is available using Secure Shell (SSH), a network security protocol for secure remote login and other secure network services over an insecure network.

Web Tools management is available through a secure browser by using Secure Sockets Layer (SSL). The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Because SSL is built into all major browsers and Web servers, installing a digital certificate turns on the SSL capabilities. For more information about Web Tools, see the *Brocade Advanced Web Tools User's Guide*.

Network manageability

The entire switch is managed as a single element and appears as a single element to a Network Management System (NMS). Each 64-port switch responds to its own IP address and appears as a separate entity to the Telnet protocol and the SNMP.

The management interfaces include blade assemblies as an intermediate component between switches and ports. In addition, all management interfaces such as, Telnet, Web Tools, the Fabric Access Layer API, and Management Server, support a "port N within blade M" naming scheme.

When SNMP devices send SNMP messages to a management console running SAN management software, the information is stored in a Management Information Base (MIB). The Fabric OS Version of the 2109 Model M12 supports the latest

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1404
3698
Doc.

Fibre Alliance Fibre Channel management (FCMGMT) MIBs, which allow common information necessary for management software to provide information to a SAN administrator.

Field replaceable units (FRUs)

Each FRU in the 2109 Model M12 is hot-swappable. Fault isolation to the FRU level provides failure containment. Each FRU can be identified remotely with the FRU part number, serial number, and revision level.

The FRUs of the the 2109 Model M12 include:

- Chassis, including backplane, blower and power supply backplane, ac harness, and blower harness (does not include blower assemblies or power supplies)
- 16-port Fibre Channel switch module
- CP
- Power supply (180 - 264 V ac, 1000 W)
- Blower assembly, including blower, control board, and housing
- Rear LED status panel cosmetic trim panel
- Chassis door
- Card slot filler panel
- Power supply filler panel
- Cable management tray
- Optical cable management guides (package of 16)
- Rack mount kit, including rear brackets and bottom support rack rails
- Optional mid-mount rack kit
- ac input cable: North America, UK, continental Europe, Australia and New Zealand, and international IEC 60309
- Serial cable
- SFP SWL transceiver
- SFP LWL transceiver

For more information about the FRUs, see the *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide.*

The CP dynamically isolates any FRU that is nonfunctional for ease of repair and replacement as well as to prevent a nonfunctional blade assembly from affecting system availability. Each switch blade assembly has 128K bits of nonvolatile memory and takes inventory of the system and determines the contents of the system electronically. For example, you can perform the following tasks:

- Determine how long components have been running when they fail
- View error logs
- View operating hours
- View log histories to determine MTBF

For more information about how to perform these tasks, see the *Brocade Fabric OS Reference.*

10472
A-

Appendix A. Product specifications

This appendix contains the 2109 Model C36 with Model M12 specifications.

2109 Model M12 components

The 2109 Model M12 contains the following components:

- A 14U chassis, designed to be mounted in a 48.26 cm (19 in.) rack. Two 2109 Model M12 switches can be mounted in a 2109 Model C36 cabinet.
- 16-port cards in configurations up to eight cards per chassis, with 16 optical ports per card, compatible with SFPs.
- Two CP cards, each with:
  - One modem serial port with a DB-9 connector (full RS-232)
  - One terminal serial port with a DB-9 connector (RS-232 signal subset)
  - One IEEE compliant RJ-45 connector for use with a 10 Mbps or 100 Mbps Ethernet connection
  - A real-time clock (RTC) with a 10-year battery and 56 bytes of NVRAM
- Four power supplies with built-in fans. The power supplies plug into internal blind-mate connectors when installed in the chassis.
- Two ac power inlet connectors with ac power switches (power panel).
- A WWN card and bezel.
- Three blower assemblies for forced-air cooling of the 16-port cards and the CP cards.

Air enters inlet vents on the blower assembly side of the chassis and exits through vents on the port side of the chassis. The blower speed is governed by inlet air temperature. The blowers go into high speed when the inlet air temperature exceeds 33°C (91°F).

Physical dimensions

The dimensions of the 2109 Model M12 are listed in Table 6.

Table 6. Physical dimensions of the 2109 Model M12

Dimension	Value
Height	14U (24.11 in.)
Depth	70.9 cm (27.9 in.)
Depth with door	72.9 cm (28.7 in.)
Width	43.7 cm (17.2 in.)

2109 Model M12 and component weights

The weight of a fully-loaded 2109 Model M12, as well as the weights of individual components, are listed in Table 7.

Table 7. Component weights

Component	Weight
Fully loaded chassis	Approximately 114 kg (250.0 lbs)
Empty chassis	47.1 kg (104.0 lbs)

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
FLS Nº 1405
3698
Doc.

Table 7. Component weights (continued)

Component	Weight
Door	3.4 kg (7.6 lbs)
Blower assembly	4 kg (8.8 lbs)
Power supply	3.2 kg (7.0 lbs)
WWN bezel	0.27 kg (0.6 lbs)
CP card	2.5 kg (5.6 lbs)
16-port card	3.9 kg (8.6 lbs)
Card filler panel	1.6 kg (3.2 lbs)
Cable management tray	0.27 kg (0.6 lbs)

2109 Model C36 with Model M12 specifications

The specifications for the 2109 Model C36 with Model M12 are listed in Table 8.

Table 8. 2109 Model C36 with Model M12 specifications

Dimension	Value
Height	1785 mm (70.3 in.)
Depth	• With rear door installed: 1042 mm (41 in.) • With rear and front door installed: 1098 mm (43.3 in.)
Width	• With side panels installed: 650 mm (25.6 in.) • Without side panel installed: 623 mm (24.5 in.)
EIA units	36 EIA units
Weight	Cabinet with two 2109 Model M12 switches: 816 kg (1795 lbs)

16-port card specifications

The ports in the 2109 Model C36 with Model M12 support full-duplex link-speeds at 2.125 Gbps or 1.0625 Gbps, inbound and outbound, automatically negotiating to the highest common speed of all the devices that are connected to the port. Each port has a SERDES that accepts 10-bit wide parallel data and serializes it into a high-speed serial stream. The parallel data is expected to be 8B/10B encoded data or equivalent.

The ports are compatible with optical SWL (780 - 850 nm), and optical LWL (1270 - 1350 nm), SFPs, and SFP-compatible cables. The strength of the signal is determined by the type of SFP being used.

The ports are universal and self-configuring, and are capable of becoming F_ports, FL_ports, or E_ports.

The ports meet all required safety standards. For more information about these standards, see Table 16 on page 23.

CP card specifications

This section describes the specifications for the CP card.

10470
A.

Memory specifications

The centralized memory maximizes switch throughput by guaranteeing full transmit and receive bandwidth to all Fibre Channel ports at all times.

Each CP card contains the type and specification of memory listed in Table 9.

Table 9. Memory specifications

Memory type	Amount
Main memory	128 MB of SDRAM (32 bits wide)
Flash memory	• User flash: 16 MB of 16-bit wide memory, stored in two 8 MB banks • Compact flash: 256 MB, partitioned in two 128 MB sections
Boot flash memory	512 KB of 8-bit wide memory for system startup

Battery specifications

The CP card has a lithium carbon-monoflouride coin cell battery.

Table 10 lists the battery specifications.

Table 10. Battery specifications

Type	Specification
Rayovac BR1225	3.0 volt, 50 mAh

CAUTION:
There is a danger of explosion if the battery is incorrectly replaced. All used batteries must be discarded according to the manufacturer's instructions. Contact IBM if the real time clock begins to lose time (4)

Terminal serial port specifications

Each CP card provides a terminal serial port with a DB-9 connector with an RS-232 signal subset.

Note: For dust and electrostatic discharge (ESD) protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

You can use the terminal serial port to connect to a computer workstation or terminal without connecting to the fabric. Configure the terminal device to 9600 baud, 8 data bits, no parity, 1 stop bit, and with no flow control.

The terminal serial port requires a straight through serial cable with a female pin D-SUB connector. Use the pinouts listed in Table 11.

Table 11. Terminal serial port pinouts

Pin	Signal	Description
1		
2	Exudate	Transmit data
3	Rewaxed	Receive data
4		

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1406
3698
Doc.

Table 11. Terminal serial port pinouts (continued)

Pin	Signal	Description
5	AND	Logic ground
6		
7		
8		
9		

Modem serial port specifications

Each CP card has a modem serial port with a fully RS-232 compliant DB-9 connector.

Note: For dust and END protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

Use the modem serial port to attach a modem to each CP card. The 2109 Model M12 detects modems only during the power-on or restart sequences, and automatically initializes them for operation. If modems are connected to an operating switch, a power on and off cycle, restart, or fast restart is required in order to detect the modems.

You should connect a "Y." cable on the telephone line to each modem. The active CP card answers on the first ring. The standby CP card answers on the seventh ring if the active CP card fails to answer.

The modem serial port pinouts are listed in Table 12.

Table 12. Modem serial port pinouts

Pin	Signal	Description
1	DCD	
2	Rewaxed	Receive data
3	Exudate	Transmit data
4	DTR	Data term ready
5	AND	Logic ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

Facility specifications

To ensure correct operation of the 2109 Model C36 with Model M12 , ensure that the facility meets the following specifications:

- Power requirements for a physical inlet:
  - Input power requirements: 200 - 240 V ac, AA 50 - 60 Hz
  - Recommended power connector
- An adequate supply circuit, line fusing, and wire size, according to the electrical rating on the switch nameplate.

- An air flow of at least 350 cubic feet per minute per switch, available in the immediate vicinity of the 2109 Model C36 with Model M12.
- The power specifications listed in "Power specifications".
- The environmental specifications listed in "Environmental requirements" on page 22.
- Interference less than the standard levels listed in Table 15 on page 22, under Immunity.

Power specifications

CAUTION:
To remove power to the 2109 Model M12, disconnect both power cables. (5)

The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections and distributed name server (DNS). It is electro-magnetic compatibility (EMC) compliant.

The power supplies are universal and capable of functioning worldwide without using voltage jumpers or switches. They meet IEC 61000-4-5 surge voltage requirements and are autoranging in terms of accommodating input voltages and line frequencies. Each power supply has its own built-in fan for cooling, pushing the air towards the port side of the chassis.

The power specifications listed in Table 13 are calculated for fully-loaded systems with four power supplies. A fully-loaded system has eight 16-port cards, two CP cards, and three blower assemblies.

Table 13 lists the power specifications for the 2109 Model C36 with Model M12.

Table 13. Power specifications

Specification	Value
Total power available from each power supply	1 KW
Input voltage	200 - 240 V ac
Input line frequency	50 - 60 Hz
Harmonic distortion	Active power factor correction per IEC1000-3-2
Heat output (BTU rating)	• 64 ports: 1080 watts, 3690 BTU per hour • 128 ports : 1960 watts, 6700 BTU per hour
Maximum inrush current per power cord	40 amps Peak
Input line protection	Thermal circuit breaker
Power supply dimensions	6.96 cm (2.74 in.) wide, 12.34 cm (4.86 in.) high, 34.29 cm (13.50 in.) long

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1407
Doc 3698

Environmental requirements

Table 14 lists the environmental operating ranges for the 2109 Model C36 with Model M12. The requirements for non-operating conditions are also provided for acceptable storage and transportation environments.

Table 14. Environmental requirements

Condition	Acceptable range during operation	Acceptable range during nonoperation
Temperature (See Note)	0° - 40°C (40° - 104°F)	0° - 40°C (40° - 104°F)
Humidity	20% - 80% RH noncondensing, at 40°C	0% - 90% RH noncondensing, at 40°C
Altitude	0 - 3 km (0 - 10 000 ft) above sea level	0 - 12 km (0 - 39 370 ft) above sea level
Shock	4G, 11 MS duration, half-sine wave	0G, 11 MS duration, sq wave
Vibration	5G, 0 - 3 kHz at 1.0 octave per minute	10G, 0 - 5 kHz at 1.0 octave per minute
Heat dissipation	• 64 ports: 3690 BTU per hour • 128 ports: 6700 BTU per hour	Not applicable
Note: Temperature measured at the air inlets on the blower assembly side of the chassis.		

General specifications

Table 15 lists the general specifications for the 2109 Model C36 with Model M12.

Table 15. General specifications

Specification	Description
Configurable port types	The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections.
EMI rating	An operating 2109 Model C36 with Model M12 conforms to the EMI radiation levels specified by the following regulations: • FCC Rules and Regulations, Part 15B, Class A level • CISPR22 Class A • EN55022 Class A • VCCI Class A ITE • AS/NZS 3548 Class A
	• CNS13438 Class A • ICES-003 Class A
System architecture	Nonblocking shared-memory switch
System processor	IBM Power PC 405GP, 200 MHz CPU
ANSI Fibre Channel protocol	FC-PH (Fibre Channel Physical and Signaling Interface standard)
Modes of operation	Fibre Channel Class 2, Class 3, and Class F
Fabric initialization	Complies with FC-SW 5.0

10466
A.

Table 15. General specifications (continued)

Specification	Description
Internet protocol (IP) over Fibre Channel (FC-IP)	Complies with FC-IP 2.3 of the FCA profile
Aggregate switch input/output (I/O) bandwidth	Per port: 4 Gbps, running at 2 Gbps, full duplex Per 16-port card: 64 Gbps, all 16 ports at 2 Gbps, full duplex
Port-to-port latency	Less than 2 microseconds with no contention (destination port is free)
Data transmission range	• Up to 500 m (1625 ft) for short wavelength optical link • Up to 10 km (32 820 ft) for long wavelength optical link
Immunity	• IEC 61000-4-2 Severity Level 3 for Electrostatic Discharge • IEC 61000-4-3 Severity Level 3 for Radiated Fields • IEC 61000-4-4 Severity Level 3 for Fast Transients • IEC 61000-4-5 Severity Level 3 for Surge Voltage • IEC 61000-4-6 Conducted Emissions • IEC 61000-4-11 Voltage Variations
Acoustics	When measured in EIA 4 of a 36 EIA TotalStorage rack, with front cover, and rear cover with acoustic baffle, declared sound power is LwAd = 7.5 B, average bystander sound pressure is LpA = 59 dBA.
Routing capacity	A minimum aggregate routing capacity of four million frames per second is provided for Class 2, Class 3, and Class F frames in a 64–port switch.

Regulatory specifications

The 2109 Model M12 is certified for the regulatory specifications that are listed in Table 16.

Table 16. Regulatory specifications

Country or region	Safety specification	EMC specification
Canada	CSA 22.2 No. 60950 Third Ed.	ICES-003 Class A
United States	UL 60950 Third Ed., Info. Tech. Equip.	FCC Part 15, Subpart B, (CFR title 47) Class A
Japan	IEC 60950+A1+A2+A3+A4+A11	VCCI V-3/2000.04, Class A
International	IEC 60950+A1+A2+A3+A4+A11	CISPR22 Class A

CPMI – CORREIOS
Fls. Nº 1408
3698
Doc.

Table 16. Regulatory specifications (continued)

Country or region	Safety specification	EMC specification
Norway	Nemko IEC 60950+A1+A2+A3+A4+A11 (CB Report)	
European Union (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom)	73/23/EEC based on compliance to EN 60950:92 +A1:93+A2:93+A3:95+ A4:96+A11:97 (CB report inclusive of county deviations); TUV-GS (Germany)	89/336/EEC EN 55022:1998 Class A EN 55024 (Immunity EN 60825-1:1994/A11, -2 EN 61000-4-2 Severity Level 3 for Electro Static Discharge EN 61000-4-3 Severity Level 3 for Radiated Fields EN 61000-4-4 Severity Level 3 for Electrical Fast Transients EN 61000-4-5 Severity Level 3 for Surge Voltage EN 61000-4-6 Conducted Emissions EN 61000-4-8 Magnetic Fields EN 61000-4-11 Line Interruption
Taiwan		BSMI Certification CNS 13438
Australia and New Zealand		AS/NZS 3548:1995 Class A (radio interference)

The 2109 Model C36 is certified for the following regulatory specifications:

- IEC 60950/EN 60950 Third Ed.
- CSA 60950-00/ANSI-UL 60950 Third Ed.
- CE (7/23/EEC based on EN 60950 Third Ed.; 89/336/EEC)

Appendix B. Safety certifications and regulatory compliance

The switch complies with all the safety and regulatory standards listed in this chapter.

Safety

The switch is certified to:

- UL1950/CSA950 binational
- IEC950/EN 60950 (Nemko & TUV; CE)

Additionally, the following Product Safety/Country or Region Testing/Certifications has been completed.

- Federal Communications Commission (FCC) statement (United States)
- Voluntary Control Council for Interference (VCCI) mark (Japan)
- BSMI (Taiwan)
- C-tick mark (Australia)
- CE Mark (Europe)
- Canada class number
- GOST approval (Russia)
- NOM mark (Mexico)

EMI/EMC

Radiated Electromagnetic Interference (EMI) emissions for the power supply operating in a single or redundant power configuration comply with EMI levels specified by the following regulations:

- Electromagnetic Compatibility (EMC) Directive 89/336/EEC and the Complementary Directives 92/31/EEC and 93/68/EEC
- Low Voltage Directive (LVD) 73/23/EEC and the Complementary Directive 93/68/EEC
- FCC Docket No. 20780, Part 15J, Class B level
- CISPR22 Class A
- EN55022 Class B
- VCCI Class A ITE

Additionally, the power supply has received a CE Mark for susceptibility and complies with the following Electromagnetic Compatibility (EMC) regulations:

- EN50082-2/EN55024:1998 (European Immunity Requirements)
  - EN 61000-3-2 (Harmonics)
  - EN 61000-3-3 (Voltage Fluctuations)
  - EN 55024 (Immunity)

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1409
3698
Doc.

Immunity

The switch provides immunity 50% greater than the levels that EN 55024 specifies and complies with the following specifications:

- EN 61000-4-2, Severity Level 3 for ESD
- EN 61000-4-3, Severity Level 3 for RF Fields
- EN 61000-4-4, Severity Level 3 for EFT/Burst
- EN 61000-4-5, Severity Level 3 for Surge Voltage
- EN 61000 4-11, Power, Sag, Dip, and Variations

10462
A.

Appendix C. Danger and caution notice translations

Arabic

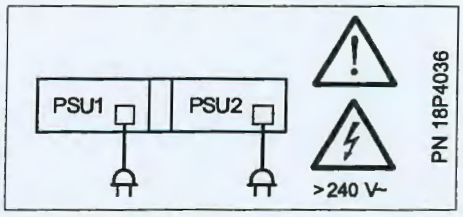
ملاحظات الأمان

تم طباعة ملا حظات الأمان في هذا الكتاب.

- تحذر ملاحظات الخطر من الظروف أو الإجراءات التي تتسبب في حدوث وفاة أو إصابة الشخص إصابة خطيرة.
- تحذر ملاحظات التحذير من الظروف أو الإجراءات التي قد تتسبب في إصابة الشخص إصابة ثانوية أو غير قاتلة.
- تحذر ملاحظات الإنتباة من الظروف أو الإجراءات التي قد تتسبب في حدوث أضرار للماكينات والأجهزة والبرامج.

قم باستخدام الأرقام بين الأقواس، مثلا (١)، في نهاية كل ملاحظة للوصول للترجمة المنشودة.

تحذير:
قد تحتوي هذه الوحدة على سلكين لإزالة كل الطاقة قم بفصل كلا من السلكين.(1)



تحذير:
قم باستخدام وحدات GBIC فقط في الولايات المتحدة الأمريكية أو منتجات من الألياف البصرية والتي تتفق مع معايير FDA الخاصة بأداء الإشعاع، 21 CFR Subchapter J. أما دوليا، يتم استخدام فقط وحدات GBIC أو منتجات من الألياف البصرية والتي تتفق مع معايير IEC 825-1. قد تتسبب المنتجات البصرية في ضوء ينطوي على خطر على العين. (2)

SJ000338

تحذير:
من الممكن أن تتسبب بطارية الليثيوم في حدوث حريق أو انفجار أو حروق خطيرة.
لا تقم باعادة شحنها أو فكها أو تسخينها لأكثر من ١٠٠ (٢١٢) أو اللحام مباشرة الى البطارية أو تقبها أو تعريض محتوياتها للماء. تحفظ بعيدا عن الأطفال. يتم استبدالها فقط برقم الجزء المحدد للنظام الخاص بك. قد ينطوي استخدام بطارية أخرى على مخاطرة حدوث حريق أو انفجار. ينطوي موصل البطارية على شحنة كهربائية، لا تحاول عكس هذه الشحنة. يتم التخلص من البطارية وفقا للقوانين المحلية (3)

SJARA347

ÊÍÐíÜÜÑ:
íÍÊãá ÎÏæË ÇäÝÌÇÑ ÇÐÇ Êã ÇÓÊÈÏÇá ÇáÈØÇÑíÉ ÈØÑíÞÉ ÛíÑ ÕÍíÍÉ.
íÌÈ ÇáÊÎáÓ ãä ÌãíÚ ÇáÈØÇÑíÇÊ ÇáÞÏíãÉ ØÈÞÇ áÊÚáíãÇÊ ÌåÉ ÇáÊÕäíÚ.
ÇÊÕá ÈÔÑßÉ IBM Úäï ÈÏÁ ÎÏæË Ãí ÊÃÎíÑ Ýí æÞÊ ÓÇÚÉ real time clock (4)

ÊÍÐíÜÜÑ:
Þã ÈÝÕá ÇáØÇÞÉ ÇáÍÇÔÉ ÈÜ 2109 Model M12 ¡ Þã ÈÝÕá ÇáßÇÈáííä ÇáÎÇÕííä ÊÇáØÇÞÉ.

SJARA699

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
1410
Fls. Nº
3698
Doc.

Brazilian-Portuguese

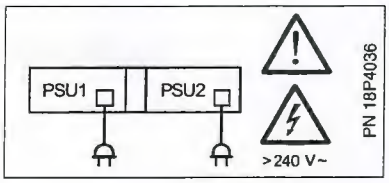
Avisos sobre Segurança

Avisos sobre segurança estão impressos em toda esta publicação.

- Um aviso de *Perigo* adverte sobre condições ou procedimentos que podem resultar em morte ou ferimentos graves.
- Um aviso de *Cuidado* adverte sobre condições ou procedimentos que podem causar ferimentos não-fatais nem extremamente graves.
- Um aviso de *Atenção* adverte sobre condições ou procedimentos que podem causar danos a máquinas, equipamentos ou programas.

Utilize os números de referência entre parênteses, como por exemplo (1), no final de cada aviso, para estabelecer uma relação com a tradução desejada.

CUIDADO:
Esta unidade pode ter dois cabos de alimentação. Para remover toda a energia, desconecte os dois cabos de alimentação. (1)



CUIDADO:
Nos EUA utilize apenas unidades GBIC ou produtos de Fibra Ótica que estejam em conformidade com as normas de desempenho de radiação da FDA, CFR 21 Subcapítulo J. Internacionalmente, utilize apenas unidades GBIC e produtos de Fibra Ótica que estejam em conformidade com a norma IEC 825-1. Produtos óticos que não estejam em conformidade com essas normas podem produzir luz prejudicial aos olhos. (2)

SJBRA338

CUIDADO:
Uma bateria de lítio pode causar fogo, explosão ou queimadura grave. Não recarregue, desmonte, aqueça acima de 100°C (212°F), utilize solda diretamente na bateria, incinere ou exponha o conteúdo da bateria à água. Mantenha longe de crianças. Substitua apenas pelo número de peça especificado para seu sistema. O uso de outra bateria pode apresentar risco de fogo ou explosão. O conector da bateria é polarizado; não tente inverter a polaridade. Descarte a bateria de acordo com as regulamentações locais. (3)

SJBRZ347

ATENÇÃO:
Existe perigo de explosão se a bateria não for substituída corretamente. Todas as baterias usadas devem ser descartadas de acordo com as instruções do fabricante.
Entre em contato com a IBM se o relógio de tempo real começar a atrasar. (4)

ATENÇÃO:
Para remover a energia do 2109 Modelo M12, desconecte ambos os cabos de alimentação. (5)

SJBRA699

Chinese, simplified

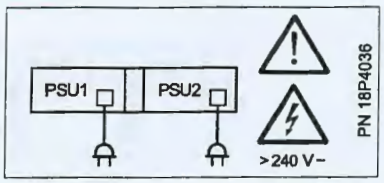
安全声明

安全声明贯穿打印在此书中。

- 危险声明警告您那些可能导致死亡或严重人身伤害的状况或过程。
- 小心声明警告您那些可能导致非致命或严重危险的人身伤害的状况或过程。
- 注意声明警告您那些可能导致损坏机器、设备或程序的状况或过程。

请使用每个声明后圆括号中引用号，例如（1），匹配查找希望的翻译。

小心:
此单元可能有两条电源软线。要除去所有电源，请断开连接两条电源软线。(1)



注意:
在美国仅使用遵守 FDA 辐射性能标准 21 CFR 子章节 J 的 GBIC 单元或光纤产品。国际上，仅使用遵守 IEC 标准 825-1 的 GBIC 单元和光纤产品。不遵守这些标准的光学产品可能会产生对眼睛有害的光线。(2)

SJ000338

注意:
锂电池可能会起火、爆炸或剧烈燃烧。不要对电池充电、分解或加热超过摄氏 100 度（华氏 212 度）、在电池上直接焊接、焚烧或请将电池内含物暴露在水中。使电池远离儿童。请仅用专为系统指定的部件号替换。使用其它电池可能面临失火或爆炸的危险。电池连接器是有极性的；请勿尝试倒转其极性。请按照本地规章废弃电池。(3)

SJCHS347

警告:
如果错误地更换了电池，则有爆炸的危险。所有用过的电池必须根据制造商的说明来废弃。如果实时时钟开始变慢，则请与 IBM 联系。（4）

警告:
要卸下 2109 M12 型的电源，请将两根电源电缆都断开。（5）

SJCHS699

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1411
Doc 3698

10459
4.

Chinese, traditional

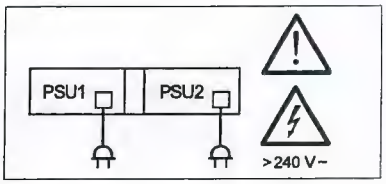
安全注意事項

此書皆為安全注意事項。

- *危險*注意事項是為了提醒您一些會導致死亡或嚴重個人傷害的情況。
- *警告*注意事項是為了提醒您一些不致構成生命危險但會造成個人傷害的情況。
- *一般*注意事項是為了提醒您一些會造成機器、設備或程式損毀的情況。

請利用每一注意事項後面括弧中的參照號碼，找到您需要的語言版本，如 (1)。

警告：
此裝置可能接有兩條電線。若要切斷所有電源，請拔除這兩條電線。(1)



警告:
在美國，請使用符合 21 CFR Subchapter J (FDA 輻射標準) 的 GBIC 裝置或光纖 (Fibre-Optic) 產品。國際間，則只能使用符合 IEC 825-1 標準的 GBIC 裝置或光纖 (Fibre-Optic) 產品。 未符合這些標準的光學產品可能會產生對眼睛造成嚴重傷害的光線。 (2)

SJ000338

警告:
鋰電池會引起火災、爆炸，以及嚴重的燒傷。 請勿將電池再充電、拆卸、加熱超過攝氏 100 度 (華氏 212 度)、直接對電池焊接、焚化，或將電池內容物曝露於水中。 勿讓孩童接近。 更換電池時，請以您系統所指定的產品編號更換。若使用別種電池，可能會引起火災或爆炸的危險。 電池兩極具有極性，請依照規定裝置，勿倒置。請依照當地相關規定處理廢棄電池。(3)

SJTAI347

注意：
如果更換電池的方法不正確，可能會有爆炸的危險。所有使用過的電池，必須按照製造商的指示來棄置。若發現即時鐘開始變慢，請與 IBM 連絡。(4)

注意：
在關閉 2109 機型 M12 電源之前，請先拔除這兩條電源線。(5)

SJTAI699

10458

Croatian

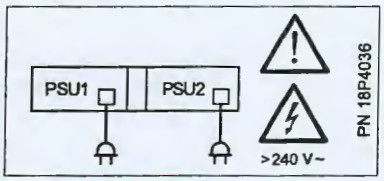
Napomene o sigurnosti

Napomene o sigurnosti su ispisane u cijeloj ovoj knjizi.

- Napomene o opasnosti vas upozoravaju na uvjete ili procedure koji mogu rezultirati sa smrtnim slučajem ili ozbiljnim osobnim povredama.
- Napomene za oprez vas upozoravaju na uvjete ili procedure koji mogu uzrokovati osobnu povredu koja nije posebno ili smrtno opasna.
- Napomene za pažnju vas upozoravaju na uvjete ili procedure koji mogu uzrokovati štetu na strojevima, opremi ili programima.

Upotrebite brojeve u zagradama, na primjer (1), na kraju svake napomene da uparite željeni prijevod.

OPREZ:
Ova jedinica može imati dva priključna kabela. Da isključite sva napajanja, odspojite oba naponska kabla. (1)



OPREZ:
U Sjedinjenim Državama koristite samo GBIC jedinice ili proizvode s optičkim vlaknima koji su u skladu s FDA standardima za zračenje, 21 CFR Subchapter J. Internacionalno koristite samo GBIC jedinice ili proizvode s optičkim vlaknima koji su u skladu s IEC standardom 825-1. Optički proizvodi koji nisu u skladu s tim standardima mogu proizvesti svjetlo koje je opasno za oči. (2)

SJ000338

OPREZ:
Litijska baterija može uzrokovati vatru, eksploziju ili ozbiljne opekotine. Nemojte ju ponovo puniti, rastavljati, zagrijavati iznad 100 stupnjeva C (212 stupnjeva F), spajati izravno na ćelije, spaljivati ili stavljati sadržaj ćelija u vodu. Držite daleko od djece. Zamijenite samo s brojem dijela koji je naveden za vaš sistem. Upotreba drukčije baterije može predstavljati rizik od vatre ili eksplozije. Konektor baterije je polariziran; ne pokušavajte promijeniti polaritet. Odbacite bateriju na način koji je u skladu s lokalnim propisima. (3)

SJCRO347

OPREZ:
Postoji opasnost od eksplozije ako se baterija pogrešno zamjenjuje.
Sve iskorištene baterije se moraju odbaciti u skladu s uputama proizvođača.
Kontaktirajte IBM ako sat za stvarno vrijeme počne kasniti. (4)

OPREZ:
da uklonite napajanje za 2109 Model M12, odspojite oba kabla za napajanje. (5)

SJCRO699

RQS nº 09/2005 - CN
CPMI - CORREIOS
1112
Fls Nº
Doc 3698

Czech

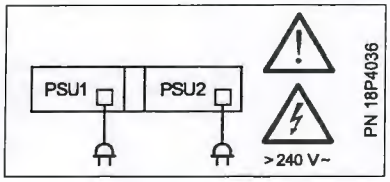
Bezpečnostní pokyny

Tato kniha obsahuje řadu bezpečnostních pokynů.

- Instrukce *Nebezpečí* upozorňuje na podmínky nebo procedury, které mohou způsobit smrt nebo vážný úraz.
- Instrukce *Pozor* upozorňuje na podmínky nebo procedury, které mohou způsobit úraz (ani smrtelný, ani vážný).
- Instrukce *Upozornění* upozorňuje na podmínky nebo procedury, které mohou způsobit poškození strojů, zařízení nebo programů.

Pro nalezení překladu bezpečnostní instrukce použijte referenční číslo v závorkách na konci této instrukce, např. (1).

POZOR:
Jednotka může mít dvě napájecí šňůry. Pro odstranění napájení odpojte obě šňůry. (1)



POZOR:
V USA používejte pouze jednotky GBIC nebo produkty na bázi optických vláken odpovídající standardům FDA radiation performance standards, 21 CFR Subchapter J. V ostatních zemích používejte pouze jednotky GBIC nebo produkty na bázi optických vláken odpovídající standardům IEC standard 825-1. Produkty na bázi optických vláken, které těmto standardům neodpovídají, mohou vydávat očím nebezpečné záření. (2)

SJ000338

POZOR:
Lithiová baterie může způsobit požár, výbuch nebo vážné popálení. Vyvarujte se nabíjení, rozebírání, zahřívání nad 100 stupňů Celsia (212 F), pájení přímo do článku, zapalování nebo styku obsahu článku s vodou. Odstraňte z dosahu dětí. Nahrazujte pouze součástkou s číslem součástky uvedenýmpro váš systém. Použitím jiné baterie riskujete požár nebo výbuch. Konektor baterie je polarizovaný; nepokoušejte se polaritu obrátit. Baterie likvidujte v souladu s místními předpisy. (3)

SJCZE347

POZOR:
Pokud je baterie nesprávně vyměněna, hrozí nebezpečí výbuchu. Použité baterie musí být zlikvidovány dle pokynů výrobce. Pokud se začíná opožďovat ukazatel reálného času (hodiny), kontaktujte IBM. (4)

POZOR:
Abyste odpojili 2109 Model M12 od napájení, musíte odpojit oba napájecí kabely. (5)

SJCZE699

10 456
A

Danish

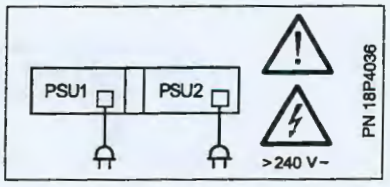
Sikkerhedsforskrifter

Denne vejledning indeholder udelukkende sikkerhedsforskrifter.

- Sikkerhedsforskrifter mærket Fare! advarer om forhold, der kan være livsfarlige eller forårsage alvorlige ulykker.
- Pas på! advarer om forhold, der kan være farlige.
- Bemærk! advarer om forhold eller procedurer, der kan forårsage skade på maskiner, udstyr eller programmer.

Brug nummeret i parentes, f.eks. (1), efter hver sikkerhedsforskrift til at finde den tilsvarende engelske tekst.

Pas på!
Enheden kan have to netledninger. Tag begge ledninger ud for at afbryde al strømforsyning. (1)



Pas på!
I USA må der kun bruges GBIC-enheder eller fiberoptiske produkter, der overholder FDA-strålingsstandarderne, 21 CFR Subchapter J. I andre lande må der kun bruges GBIC-enheder eller fiberoptiske produkter, der overholder IEC-standard 825-1. Optiske produkter, som ikke overholder disse standarder, kan udsende lys, der er skadeligt for øjnene. (2)

SJ000338

Pas på!
Litiumbatteriet kan forårsage brand eller eksplosion og give alvorlige brandsår. Det må ikke genoplades, åbnes, udsættes for mere end 100 grader celsius, brændes eller komme i berøring med vand. Batteriet skal opbevares utilgængeligt for børn. Det må kun udskiftes med et litiumbatteri, der har det partnummer, der er angivet til systemet. Der er fare for eksplosion eller brand, hvis der benyttes andre batterityper. Batteriet har to poler, der ikke må byttes om. Batteriet skal kasseres i henhold til de lokale bestemmelser. Spørg kommunens tekniske forvaltning (miljøafdelingen). (3)

SJDAN347

Pas på!
Batteriet kan eksplodere, hvis det ikke udskiftes korrekt. Alle brugte batterier skal bortskaffes i overensstemmelse med gældende miljøbestemmelser. Kontakt IBM, hvis systemuret begynder at tabe tid. (4)

Pas på!
Afmontér begge netledninger for at fjerne al strømforsyning til model 2109-M12. (5)

SJDAN699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1449
Doc 3698

Finnish

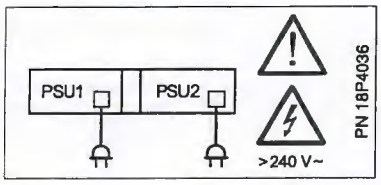
Turvaohjeet

Tähän kootut turvaohjeet toistuvat tämän julkaisun asianmukaisissa kohdissa.

- *VAARA*-ilmaisua (DANGER) käytetään varoittamaan hengenvaarallisesta tai vakavan ruumiinvamman aiheuttavasta tilanteesta.
- *Varoitus* (CAUTION) tarkoittaa, että kyseinen tilanne saattaa aiheuttaa henkilölle kohtalaisia tai vähäisiä vammoja.
- *Huomio* (Attention) tarkoittaa, että kyseinen tilanne saattaa vahingoittaa konetta, laitetta tai ohjelmia.

Kunkin turvaohjeen perässä on sulkeissa numero, esimerkiksi (1), jonka avulla englanninkielistä ohjetta vastaava suomenkielinen ohje löytyy kätevästi.

Varoitus:
Tässä yksikössä voi olla kaksi verkkojohtoa. Katkaise virransyöttö irrottamalla molemmat verkkojohdot. (1)



Varoitus:
Yhdysvalloissa saa käyttää vain GBIC-yksiköitä tai kuituoptisia tuotteita, jotka täyttävät elintarvike- ja lääkevalvontaviraston (FDA) säteilystandardin 21 CFR Subchapter J vaatimukset. Muissa maissa tulee käyttää vain standardin IEC 825-1 mukaisia GBIC-yksiköitä tai kuituoptisia tuotteita. Optiset tuotteet, jotka eivät ole näiden standardien mukaisia, saattavat tuottaa silmiä vahingoittavaa valoa. **(2)**

SJ000338

Varoitus:
Litiumparisto voi aiheuttaa tulipalon tai palovammoja tai se voi räjähtää, ellei seuraavia ohjeita noudateta: Älä yritä ladata paristoa tai purkaa sitä osiin. Älä kuumenna paristoa yli 100 Celsius-asteen lämpötilaan äläkä hävitä sitä polttamalla. Älä juota paristoon mitään. Älä päästä pariston sisältöä kosketukseen veden kanssa. Pidä paristo poissa lasten ulottuvilta. Pariston saa vaihtaa vain paristoon, joka on osanumeron perusteella tarkoitettu kyseiseen järjestelmään. Muuntyyppisen pariston käyttö voi aiheuttaa tulipalon tai räjähdyksen. Pariston liitin on muotoiltu niin, että sen napaisuus on oikea, kun paristo asetetaan asianmukaisesti. Älä aseta paristoa väärin päin. Hävitä paristo ongelmajätteistä säädettyjen lakien ja viranomaisten määräysten mukaisesti. (3)

SJFIN347

POZOR:
Pokud je baterie nesprávně vyměněna, hrozí nebezpečí výbuchu. Použité baterie musí být zlikvidovány dle pokynů výrobce. Pokud se začíná opožďovat ukazatel reálného času (hodiny), kontaktujte IBM. (4)

POZOR:
Abyste odpojili 2109 Model M12 od napájení, musíte odpojit oba napájecí kabely. (5)

SJFIN699

10454

A

French

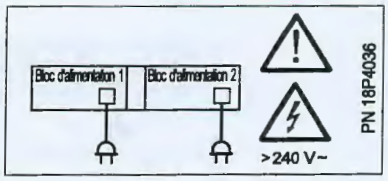
Consignes de sécurité

Les consignes de sécurité s'appliquent à l'ensemble du présent manuel.

- Les consignes de sécurité de type *DANGER* indiquent la présence d'un risque de blessure grave ou mortelle.
- Les consignes de sécurité de type *ATTENTION* indiquent la présence d'un risque de blessure légère.
- Les consignes de type *AVERTISSEMENT* indiquent la présence d'un risque d'endommagement de machines, de matériel ou de programmes.

Aidez-vous des numéros entre parenthèses, par exemple : (1), à la fin de chaque note, pour retrouver la traduction correspondante.

ATTENTION
Cette unité peut être équipée de deux cordons d'alimentation. Pour supprimer toutes les tensions dans l'unité, débranchez les deux cordons. (1)



ATTENTION
Aux Etats-Unis, seules les unités GBIC ou les produits à fibre optique conformes aux normes FDA sur les radiations (21 CFR Sous-chapitre J) peuvent être utilisés. Dans les autres pays, seuls les unités GBIC ou les produits à fibre optique conformes à la norme CEI 825-1 peuvent être employés. Les produits à fibre optique non conformes à ces normes peuvent émettre de la lumière dangereuse pour les yeux. (2)

SJ000338

ATTENTION
Prenez garde aux risques d'incendie, d'explosion ou de brûlures graves liés à l'utilisation d'une pile au lithium. Ne rechargez pas la pile et ne la démontez pas. Ne l'exposez pas à une température supérieure à 100 °C, ne la soudez pas, ne la faites pas brûler et n'en exposez pas le contenu à l'eau. Gardez la pile hors de portée des enfants. Si vous la remplacez, commandez une pile de rechange de même référence. Toute autre pile risquerait de prendre feu ou d'exploser. Le connecteur de la pile est polarisé. N'essayez pas d'inverser la polarité. Ne mettez pas la pile à la poubelle. Pour le recyclage ou la mise au rebut, reportez-vous à la réglementation en vigueur. (3)

SJFRE347

ATTENTION :
Il existe un risque d'explosion en cas de remplacement incorrect de la pile. Toutes les piles usées doivent être mises au rebut selon les instructions du fabricant. Contactez IBM lorsque l'horloge temps réel se met à retarder. (4)

ATTENTION :
Pour couper l'alimentation du 2109 Modèle M12, débranchez les deux cordons d'alimentation. (5)

SJFRA699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1414
Doc 3698

German

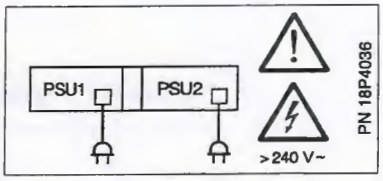
Sicherheitshinweise

Dieses Buch enthält Sicherheitshinweise.

- Die Nichtbeachtung der Vorschriften in den mit VORSICHT gekennzeichneten Sicherheitshinweisen kann zu schweren Verletzungen oder sogar zum Tod führen.
- Die Nichtbeachtung der Vorschriften in den mit ACHTUNG gekennzeichneten Sicherheitshinweisen kann zu leichten Verletzungen bzw. zu Schäden an Hardware oder Software führen.

Verwenden Sie die Referenznummern in Klammern, beispielsweise (1) am Ende der einzelnen Sicherheitshinweise, um die gewünschte Übersetzung zu bekommen.

ACHTUNG
Diese Einheit könnte zwei Stromversorgungskabel haben. Um die Einheit ganz von der Netzspannung zu trennen, beide Stromversorgungskabel lösen. (1)



ACHTUNG:
Nur GBIC-Einheiten oder Glasfaserpr odukte verwenden, die dem IEC Standard 60825-1 entsprec hen. Optisc he Produkte , die diesen Standar ds nic ht entsprec hen, können Strahlung en erzeugen, die zu A ugenverletzung en führen können. (2)

SJGER338

ACHTUNG:
Lithiumbatterien sind feuergefährlich, explosiv und können schwere Verbrennungen verursachen. Batterie nicht wiederaufladen, öffnen oder über 100 Grad Celsius erhitzen; die Zelle nicht direkt anlöten, verbrennen oder den Inhalt der Zelle mit Wasser in Berührung bringen. Batterie nicht in Reichweite von Kindern aufbewahren. Eine verbrauchte Batterie nur durch eine Batterie mit der für dieses System spezifizierten Teilenummer ersetzen. Andere Batterien können sich entzünden oder explodieren. Der Batterieanschluss hat zwei verschiedene Pole; beim Anschließen die Pole nicht vertauschen. Batterie gemäß den örtlichen Richtlinien für Sondermüll entsorgen. (3)

SJGER347

Achtung:
Die Batterie kann bei unsachgemäßem Austauschen explodieren. Batterien nach Gebrauch als Sondermüll entsorgen. Kontakt mit IBM aufnehmen, wenn der Taktgeber nicht mehr korrekt funktioniert. (4)

Achtung:
Beide Netzkabel von der Stromversorgung trennen, um das 2109 Modell M12 von der Stromversorgung zu trennen. (5)

SJGER699

10452

A-

Greek

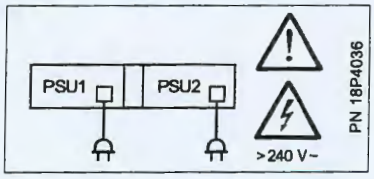
Σημειώσεις ασφάλειας

Σε αυτό το εγχειρίδιο υπάρχουν σημειώσεις ασφάλειας.

- Οι σημειώσεις κινδύνου προειδοποιούν για συνθήκες ή διαδικασίες που θα μπορούσαν να προκαλέσουν θάνατο ή σοβαρό τραυματισμό.
- Οι σημειώσεις προσοχής προειδοποιούν για συνθήκες ή διαδικασίες που θα μπορούσαν να προκαλέσουν τραυματισμό, όχι θανατηφόρο ούτε εξαιρετικά επικίνδυνο.
- Οι σημειώσεις επισήμανσης προειδοποιούν για συνθήκες ή διαδικασίες που θα μπορούσαν να προκαλέσουν ζημίες σε μηχανές, εξοπλισμό ή προγράμματα.

Χρησιμοποιείτε τους αριθμούς αναφοράς σε παρένθεση στο τέλος κάθε σημείωσης, π.χ. (1), για να βρείτε την αντίστοιχη μετάφραση.

ΠΡΟΣΟΧΗ:
Αυτή η μονάδα μπορεί να έχει δύο καλώδια γραμμής. Για να διακόψετε πλήρως την παροχή ρεύματος, αποσυνδέστε και τα δύο καλώδια γραμμής. (1)



ΠΡΟΣΟΧΗ:
Στις Ηνωμένες Πολιτείες, χρησιμοποιείτε μόνο μονάδες GBIC ή προϊόντα οπτικών ινών (Fibre-Optic) που πληρούν τα πρότυπα εκπομπής ακτινοβολίας της FDA, 21 CFR Υποκεφάλαιο J. Διεθνώς, χρησιμοποιείτε μόνο μονάδες GBIC ή προϊόντα οπτικών ινών που πληρούν το πρότυπο IEC 825-1. Τα οπτικά προϊόντα που δεν πληρούν αυτά τα πρότυπα μπορεί να παράγουν φωτεινή ακτινοβολία επικίνδυνη για τα μάτια. (2)

SJGRE338

ΠΡΟΣΟΧΗ:
Μια μπαταρία λιθίου μπορεί να προκαλέσει πυρκαγιά, έκρηξη ή σοβαρά εγκαύματα. Μην επιχειρήσετε να την επαναφορτίσετε, να την αποσυναρμολογήσετε, να τη θερμάνετε πάνω από 100°C, να την αποτεφρώσετε, να πραγματοποιήσετε συγκόλληση με καλάι απευθείας στο στοιχείο ή να φέρετε τα περιεχόμενα του στοιχείου σε επαφή με νερό. Κρατήστε τη μακριά από παιδιά. Αντικαταστήστε τη μόνο με το καθορισμένο part number για το σύστημά σας. Η χρήση διαφορετικής μπαταρίας μπορεί να δημιουργήσει κίνδυνο πυρκαγιάς ή έκρηξης. Η μπαταρία συνδέεται με συγκεκριμένη πολικότητα. Μην επιχειρήσετε να αντιστρέψετε την πολικότητα. Η απόρριψη της μπαταρίας πρέπει να γίνεται σύμφωνα με τους τοπικούς κανονισμούς. (3)

SJGRE329

ΠΡΟΣΟΧΗ:
Υπάρχει κίνδυνος έκρηξης σε περίπτωση εσφαλμένης αντικατάστασης της μπαταρίας. Η απόρριψη όλων των χρησιμοποιημένων μπαταριών πρέπει να γίνεται σύμφωνα με τις οδηγίες του κατασκευαστή. Επικοινωνήστε με την IBM αν το ρολόι πραγματικού χρόνου αρχίσει να μένει πίσω. (4)

ΠΡΟΣΟΧΗ:
Για να διακόψετε την παροχή ρεύματος στο 2109 Model M12, αποσυνδέστε και τα δύο καλώδια ρεύματος. (5)

SJGRE699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 115
Doc. 3698

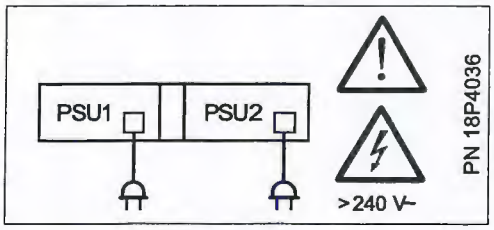
הודעות בטיחות

הודעות בטיחות מודפסות לכל אורכו של ספר זה.

- הודעת סכנה מזהירה מפני מצב העלול לגרום למוות או פציעה קשה.
- הודעת זהירות מזהירה מפני מצב היכול לגרום פציעה שאינה קטלנית ואין בו סכנה קיצונית.
- הודעת ערנות מזהירה מפני מצבים או נהלים היכולים לגרום נזק למכונות, לציוד או לתוכניות.

השתמשו במספרי ההפניה בסוגריים, לדוגמה (1), בסוף כל הודעה כדי למצוא את התרגום המתאים.

זהירות:
יתכן שליחידה זו יש שני כבלי חשמל. כדי לסלק את כל החשמל, נתקו את שני כבלי החשמל (1).



זהירות

בארצות הברית, יש להשתמש רק ביחידות GBIC או מוצרי סיב-אופטי העומדים בתקני הקרינה של ה-FDA, תקן 21 CFR Subchapter J.
מחוץ לארצות הברית, יש להשתמש רק ביחידות GBIC או מוצרי סיב-אופטי העומדים בתקן IEC מס' 1 - 825. מוצרים אופטיים שאינם עומדים בתקנים אלה עלולים להפיק אור מסוכן לעיניים. (2).

SJ000338

זהירות

סוללת ליתיום עלולה לגרום לשריפה, התפוצצות או כוויה חמורה. אין לטעון אותה מחדש, לפרקה או לחמם אותה לטמפרטורה העולה על 100 מעלות צלזיוס, להלחים ישירות אל התא, לשרוף או לחשוף את תוכן התא למים. יש להרחיק את הסוללה מילדים. יש להחליף את הסוללה רק במספר החלק שצוין במערכת שלכם. השימוש בסוללה אחרת עלולה לגרום לסכנת שריפה או התפוצצות. מחבר הסוללה מקוטב; אין לנסות להפוך את הקיטוב. יש לסלק את הסוללה בהתאם לתקנות המקומיות. (3)

SJHEB347

10450
A-

זהירות:

קיימת סכנת פיצוץ אם הסוללה אינה מוחלפת כהלכה. יש לסלק את כל הסוללות המשומשות לפי הוראות היצרן. נא לפנות אל IBM במקרה ששעון זמן-האמת מתחיל לפגר. (4)

זהירות:

כדי לנתק את אספקת החשמל אל 2109 דגם M12 יש לנתק את שני כבלי החשמל. (5)

SJHEB699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1416
Doc. 3698

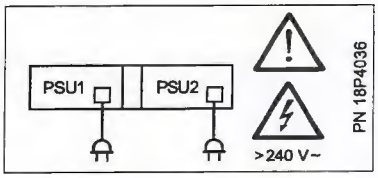
Biztonsági előírások

A biztonsági előírások a könyvben számos helyen megjelennek.

- A *Veszély* felirat figyelmeztet azokra a helyzetekre vagy eljárásokra, amelyek halált vagy súlyos testi sérülést eredményezhetnek.
- A *VIGYÁZAT* felirat olyan veszélyekre hívja fel a figyelmet,amelyek közepes vagy könnyebb személyi sérülést okozhatnak.
- A *Figyelem* felirat figyelmeztet azokra a helyzetekre vagy eljárásokra, amelyek károsíthatják a gépeket, berendezéseket vagy programokat.

Az egyes előírások végén található, zárójeben lévő hivatkozási számok, például (1), segítségével megtalálhatja a kívánt fordítást.

FIGYELEM:
Az egység két tápkábellel rendelkezik. Az áramtalanításhoz húzza ki mindké tápkábelt. (1)



Az Egyesült Államokban csak olyan GBIC egységeket vagy száloptikás termékeket használjon, amelyek megfelelnek az FDA sugárzási szabványok 21CFR J alfejezetének. Nemzetközileg csak olyan GBIC egységeket vagy száloptikás termékeket használjon, amelyek megfelelnek az IEC 825-1-es szabványának. A szabványoknak nem megfelelő optikai termékek fénye károsíthatja a szemet. **(2)**

SJ000338

VIGYÁZAT

A lítium akkumulátor tüzet, robbanást vagy súlyos égést okozhat. Ne töltse újra, ne szerelje szét, ne hevítse 100°C fölé, ne forrasszon közvetlenül a telepre, ne égesse el és ne tegye ki víz hatásának a telep tartalmát. Tartsa távol a gyermekektől. Kizárólag a rendszerhez megadott termékszámú t egységgel cserélje. Más akkumulátor használata tűz vagy robbanásveszélyes. Az akkumulátorcsatlakozó polarizált; a polaritást ne cserélje föl. A használt akkumulátort a helyi előírásoknak megfelelően kell kezelni. (3)

SJHUN347

FIGYELMEZTETÉS:
Az akkumulátor helytelen cseréje robbanásveszélyt okoz. A használt akkumulátorokat a gyártó utasításai szerint kell kezelni. Keresse meg az IBM-et, ha az óra elkezd késni! (4)

FIGYELMEZTETÉS:
Mindkét tápkábelt húzza ki, ha meg akarja szüntetni a 2109 M12 egység tápellátását! (5)

SJHUN699

10448
A.

Italian

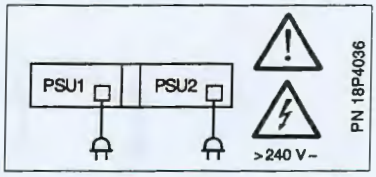
Informazioni sulla sicurezza

Le informazioni sulla sicurezza vengono stampate con questo manuale in modo completo.

- Una nota di Pericolo segnala condizioni o procedure che possono risultare estremamente dannose o pericolose per la persona.
- Una nota di Attenzione segnala condizioni o procedure che possono causare danni o lesioni personali che non sono né letali né estremamente pericolosi.
- Una nota di Avvertenza segnala condizioni o procedure che possono causare danni alle macchine, all'apparecchiatura o ai programmi.

Utilizzare i numeri di riferimento in parentesi, ad esempio (1), alla fine di ciascuna nota per ottenere la traduzione desiderata corrispondente.

AVVERTENZA:
E' possibile che questa unità sia dotata di due cavi di linea. Per rimuovere l'alimentazione, scollegare entrambi i cavi di linea. (1)



ATTENZIONE:
Negli Stati Uniti utilizzare solo unità GBIC o prodotti in fibra ottica, compatibili agli standard di radiazione FDA, 21 CFR Subchapter J.
A livello internazionale, utilizzare solo unità GBIC o prodotti in fibre ottiche compatibili con lo standard IEC 825-1. I prodotti ottici che non sono compatibili con questi standard potrebbero produrre luminosità pericolosa agli occhi. **(2)**

SJ000338

ATTENZIONE:
Una batteria a litio può causare incendio, esplosione o gravi ustioni. Non ricaricare, disassemblare, riscaldare al di sopra dei 100°C, saldare direttamente sulla cella, incenerire o esporre il contenuto delle celle in prossimità di acqua. Tenere lontano dalla portata dei bambini. Sostituire solo il numero parte specificato per il sistema. L'utilizzo di un'altra batteria potrebbe provocare un rischio di incendio o di esplosione. Il connettore della batteria è polarizzato; non tentare di invertire la polarità. Smaltire la batteria in base alle norme locali vigenti. (3)

SJITA347

ATTENZIONE:
Se la batteria non viene posizionata correttamente vi è pericolo di esplosione. Tutte le batterie usate devono essere smaltite secondo le istruzioni del produttore. Contattare l' IBM se l'orologio non è preciso. (4)

ATTENZIONE:
Per arrestare l'alimentazione del Modello M12 2109, disconnettere entrambi i cavi di alimentazione . (5)

SJITA699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1417
Nº 3698
Doc.

Japanese

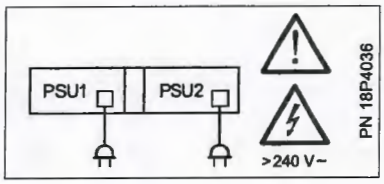
安全上の注意

安全上の注意は、本書全体にわたって印刷されています。

- 「危険」の見出しの付いている項目は、生命の危険を及ぼす、あるいは重傷を負わせる可能性のある状態または手順についての警告です。
- 「注意」の見出しの付いている注意事項は、生命の危険を及ぼすもの、あるいは非常に危険なものではないが、身体を傷つける可能性のある状態または手順についての警告です。
- 「注意」の見出しの付いている注意事項は、マシン、機器、またはプログラムに損傷を与える可能性のある状態または手順についての警告です。

それぞれの注意事項の終わりにある括弧の付いた数字、たとえば (1) を使って、必要な翻訳を選んでください。

注意
この装置には 2 つの回線コードを付けることができます。電源を完全に遮断するには、回線コードを 2 本とも外してください。(1)



注意
米国では、FDA 放射特性規定 21 CFR 副章 J に準拠する GBIC 装置または光ファイバー製品だけを使用してください。米国以外では、IEC 規定 825-1 に準拠する GBIC 装置または光ファイバー製品だけを使用してください。これらの規定に準拠していない光学式製品を使用すると、目に有害な光が出ることがあります。

(2)

SJ000338

注意
リチウム・バッテリーは火事を起こしたり、爆発したり、ひどく燃えたりすることがあります。充電したり、分解したり、100° C (212° F) 以上に熱したり、セルに直接はんだ付けしたり、焼却したり、セルの内容を水に露出したりしないでください。子供の手の届くところに置かないでください。交換する場合はご使用のシステムで決められている部品番号のものだけを使ってください。別のバッテリーを使うと火事や爆発を起こすおそれがあります。バッテリー・コネクターは分極されています。極性を逆にしないでください。バッテリーは地方自治体の規定に従って処分してください。(3)

SJJPN347

注意:
バッテリーは、正しくない方法で交換すると爆発する恐れがあります。すべての使用済みバッテリーは、製造元の指示に従って廃棄してください。もしリアルタイム・クロックが遅れるようになりましたら、IBM にご連絡ください。(4)

注意:
2109 モデル M12 への電力を除去するために、電源ケーブルを両方とも切り離してください。(5)

SJJPN699

10446
A-

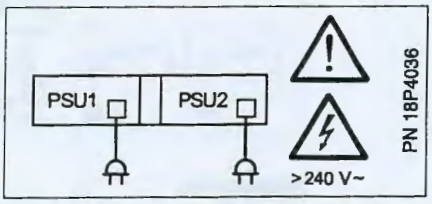
안전 정보

이 책에는 다음의 안전 정보가 표시됩니다.

- 위험사항은 사망이나 중상을 일으킬 수 있는 상태 또는 절차에 대해 경고합니다.
- 주의사항은 치명적이거나 아주 위험하지는 않은 신체적인 상해를 일으킬 수 있는 상태 또는 절차에 대해 경고합니다.
- 유의사항은 기계, 장비 또는 프로그램을 손상시킬 수 있는 상태 또는 절차에 대해 경고합니다.

각 사항의 끝에 있는 괄호 안의 참조 번호(예를 들면, (1))를 참고하십시오.

주의:
이 장치에 두 개의 전원 코드가 있을 수 있습니다. 모든 전원을 제거하려면, 두 개의 전원 코드의 연결을 모두 빼십시오. (1)



경고:
미국에서는 미식약청(FDA) 방사 성능 표준, 21 CFR 부칙 J를 준수하는 GBIC 장치나 광제품만을 사용할 수 있습니다. 국제적으로는 국제 전기 기술 위원회(IEC) 표준 825-1을 준수하는 GBIC 장치나 광제품만을 사용할 수 있습니다. 이 표준을 준수하지 않는 광제품은 눈에 해로운 광선을 방사할 수도 있습니다. (2)

SJ000338

경고:
리튬 배터리는 화재, 폭발 또는 중화상의 원인을 일으킬 수 있습니다. 리튬 배터리는 재충전하거나 해체해서는 안되며, 섭씨 100도(화씨 212도) 이상의 열에 노출시켜서는 안됩니다. 또한 셀에 직접 납땜하거나 이를 소각하지 마시고 셀 내용물이 물에 닿지 않게 하십시오. 어린이의 손에 닿지 않게 하십시오. 시스템에 지정된 부품 번호로만 교체하십시오. 다른 배터리를 사용하면 화재나 폭발을 일으킬 수도 있습니다. 배터리 커넥터는 극성을 띠고 있으므로 양극을 바꾸어 사용하지 마십시오. 지역 규정에 따라 배터리를 폐기하십시오. (3)

SJKOR347

주의:
배터리를 잘못 대체한 경우 폭발의 위험이 있습니다. 사용된 모든 배터리는 제조업체의 지시사항에 따라 폐기해야 합니다. 실시간 시계가 늦거 시작하면 IBM에 문의하십시오. (4)

주의:
2109 Model M12의 전원을 제거하려면 양쪽 전원 케이블의 연결을 모두 끊으십시오. (5)

SJKOR699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1418
3698
Doc.

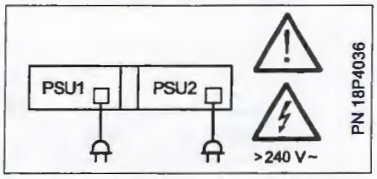
Забелешки за сигурност

Забелешките за сигурност се наоѓаат на крајот од оваа книга.

- Забелешките за опасност се однесуваат на условите и процедурите кои можат да предизвикаат повреди на пресоналот кои можат да предизвикаат смрт.
- Забелешките за внимание се однесуваат на условите и процедурите кои можат да предизвикаат повреди на пресоналот кои не се смртоносни или екстремно опасни.
- Забелешките за предупредување се однесуваат на условите и процедурите кои можат да предизвикаат штета на машините, опремата, или програмите.

Користете ги броевите во загради за референцирање, на пр.(1), на крајот на секоја забелешка за да се референцирате на саканиот превод.

ВНИМАНИЕ:
Оваа единица може да има два кабли за напојување. За да го исклучите напојувањето целосно исклучете ги двата кабли. (1)



ВНИМАНИЕ:
Во САД користете само GBIC уреди или Фибер-Оптички продукти кои ги исполнуваат FDA стандардите за радијација, 21 CFR подзагалавие J. Интернационално користете само GBIC уреди или Фибер-Оптички продукти кои го исполнуваат IEC стандардот 825-1. Оптичките продукти кои не ги исполнуваат овие стандарди може да предизвикаат светлина која е опасна за очите. (2)

SJ000338

ВНИМАНИЕ:
Литиумската батерија може да предизвика пожар, експлозија, или сериозни изгореници. Не ја полнете повторно, не ја расклопувајте, не ја загревајте над 100°C (212°F), не ја лемете директно на ќелијата, не ја палете, или не ја изложувајте содржината на ќелијата на вода. Чувајте ја подалеку од деца. Заменете ја само со дел специфициран за Вашиот систем. Користење на друга батерија претставува ризик од пожар или експлозија. Конекторот на батеријата е поларизиран, не се обидувајте да го смените поларитетот. Отстранувањето на искористените батерии се врши според локалните регулативи. (3)

SJMAC347

ВНИМАНИЕ:
Постои опасност од експлозија ако батеријата непрописно се заменува. Сите искористени батерии мора да се уништат според препораките на нивниот производувач. Контактирајте го IBM ако real time clock чипот губи информација за времето. (4)

ВНИМАНИЕ:
при исклучувањето на 2109 модел M12, исклучете ги двата мрежни (струјни) кабли. (5)

SJMKD699

10444
A.

Portuguese

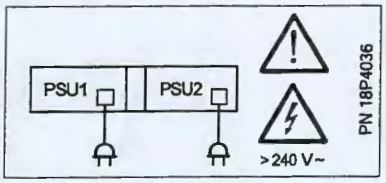
Avisos de Segurança

Os avisos de segurança encontram-se impressos ao longo deste manual.

- Um aviso de *Perigo* informa o utilizador de que há condições ou procedimentos que podem resultar em morte ou em graves danos pessoais.
- Um aviso de *Cuidado* informa o utilizador da existência de condições ou procedimentos que podem resultar em danos pessoais que não são mortais nem potencialmente perigosos.
- Um aviso de *Atenção* informa o utilizador da existência de condições ou procedimentos que podem causar danos a máquinas, equipamento, ou programas.

Recorra aos números de referência entre parêntesis (1) no final de cada aviso para saber qual a tradução pretendida.

CUIDADO:
Esta unidade poderá dispor de dois cabos eléctricos. Para cortar a alimentação desligue ambos os cabos. (1)



CUIDADO:
Nos Estados Unidos utilize apenas unidades GBIC ou produtos de Fibra-Óptica que estejam em conformidade com as normas de rendimento de radiação da FDA, 21 CFR Subcapítulo J. Internacionalmente utilize apenas unidades GBIC ou produtos de Fibra-Óptica que estejam em conformidade com a norma 825-1 da IEC. Produtos Ópticos que não estejam em conformidade com estas normas podem produzir luz que é perigosa para a vista. (2)

SJ000338

CUIDADO:
Uma pilha de lítio pode provocar fogo, explosão ou uma queimadura grave. Não recarregar, desmontar, aquecer acima dos 100°C (212°F), soldar directamente na pilha, incinerar, ou expor o conteúdo da pilha à água. Manter afastado das crianças. Substituir apenas pelo part number especificado para o sistema. A utilização de outra bateria pode apresentar um risco de fogo ou de explosão. O conector da pilha está polarizado; não tente inverter a polaridade. Deite a bateria fora de acordo com os regulamentos locais. (3)

SJPOR347

CUIDADO:
Perigo de explosão se a pilha for incorrectamente substituída.
Para deitar fora pilhas usadas, siga as instruções do fabricante.
Contacte a IBM se o relógio de tempo real começar a atrasar. (4)

CUIDADO:
Para desligar a alimentação do 2109 Modelo M12, desligue ambos os cabos de alimentação. (5)

SJPTG699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1419
Doc. 3698

10443
A

Russian

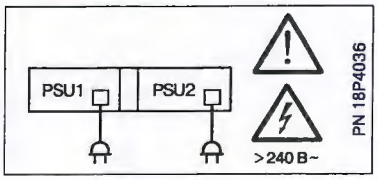
Замечания по технике безопасности

В этой книге встречаются замечания по технике безопасности.

- Замечания под заголовком *Опасно* предупреждают об условиях или операциях, которые, могут повлечь за собой смертные случаи или серьезные травмы.
- Замечания под заголовком *Осторожно* предупреждают об условиях или операциях, которые могут явиться причиной травм, но не приведут ни к смертным случаям, ни к особо серьезным поражениям.
- Замечания под заголовком *Внимание* предупреждают об условиях или операциях, которые могут привести к порче компьютеров, оборудования или программ.

Чтобы найти перевод нужного замечания, смотрите номер, указанный в скобках в конце этого замечания, например, (1).

ОСТОРОЖНО:
У этого блока может быть два шнура питания. Чтобы полностью отключить питание, отсоедините оба шнура. (1)



ОСТОРОЖНО:
В США следует применять только блоки GBIC и оптоволоконные устройства, отвечающие требованиям стандартов FDA по уровню излучения, CFR 21, подраздел J.
В других странах следует применять только блоки GBIC и оптоволоконные устройства, отвечающие требованиям стандарта IEC 825-1. Оптические устройства, не отвечающие этим стандартам, могут излучать свет, опасный для глаз. (2)

SJ000338

ОСТОРОЖНО:
Неосторожное обращение с литиевой батареей может привести к пожару, взрыву или серьезным ожогам. Не заряжайте и не разбирайте батарею, не нагревайте ее до температуры выше 100°C (212°F), не паяйте и не сжигайте ее, не допускайте контакта содержимого батареи с водой. Берегите от детей. Заменяйте только на батарею с кодом, соответствующим вашей системе. Применение другой батареи может привести к взрыву или пожару. При подключении батареи обязательно соблюдайте полярность. Утилизируйте батарею в соответствии с местным законодательством. (3)

SJRUS347

ОСТОРОЖНО:
При неправильной замене батарейки возможен взрыв. Все использованные батарейки следует утилизировать в соответствии с инструкциями изготовителя. Если часы реального времени начнут отставать, обращайтесь в IBM. (4)

ОСТОРОЖНО:
Чтобы отключить питание 2109 Model M12, отсоедините оба шнура питания. (5)

SJRUS699

10444

Slovak

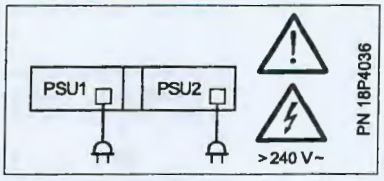
Bezpečnostné oznamy

Bezpečnostné oznamy sa nachádzajú všade v tejto knihe.

- Oznam o nebezpečenstve vás varuje pred stavmi a postupmi, ktoré môžu mať za následok smrť alebo vážne osobné zranenie.
- Výstraha vás varuje pred stavmi a postupmi, ktoré môžu spôsobiť osobné zranenie, ktoré nie je ani smrteľné ani extrémne nebezpečné.
- Upozornenie vás varuje pred stavmi a postupmi, ktoré môžu spôsobiť poškodenie strojov, zariadenia alebo programov.

Požadovaný preklad nájdete podľa referenčného čísla v zátvorkách, napríklad (1), ktoré sa nachádza na konci každého oznamu.

VÝSTRAHA:
Táto jednotka môže mať dva napájacie káble. Aby ste odstránili všetko napájanie, odpojte obidva káble. (1)



VÝSTRAHA:
V Spojených štátoch používajte len jednotky GBIC alebo optické produkty, ktoré vyhovujú radiačným štandardom FDA, 21 CFR podkapitola J.
V ostatných krajinách používajte len jednotky GBIC alebo optické produkty, ktoré vyhovujú IEC štandardu 825-1. Optické produkty, ktoré nevyhovujú týmto štandardom, môžu produkovať žiarenie, ktoré je nebezpečné pre oči. **(2)**

SJ000338

VÝSTRAHA:
Lítiová batéria môže spôsobiť požiar, výbuch alebo silné popálenie. Nedobíjajte, nerozoberajte, nezohrievajte nad 100°C, nespájkujte priamo články, nespaľujte ani nesypte obsah článkov do vody. Držte mimo dosah detí. Nahradzujte ju len batériou s číslom dielu, ktoré je uvedené pre váš systém. Použitie inej batérie môže znamenať riziko požiaru alebo výbuchu. Batéria je polarizovaná; nepokúšajte sa vymeniť polaritu. Batérie sa zbavte podľa miestnych predpisov. (3)

SJSLK347

VÝSTRAHA:
Ak je batéria nesprávne vymenená, existuje nebezpečenstvo výbuchu. Všetky použité batérie musia byť znehodnotené v súlade s pokynmi výrobcu.
Ak hodiny reálneho času začínajú meškať, obráťte sa na IBM. (4)

VÝSTRAHA:
Ak chcete odstrániť napájanie pre 2109 Model M12, odpojte obidva napájacie káble. (5)

SJSKY699

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1460
3698
Doc.

Slovenian

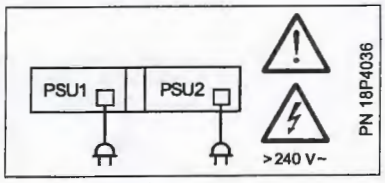
Opombe o varnosti

Opombe o varnosti so natisnjene na več mestih v tej knjigi.

- Opomba o nevarnosti vas opozarja na stanja ali postopke, ki lahko povzročijo smrt ali resne osebne poškodbe.
- Opomba o previdnosti vas opozarja na stanja ali postopke, ki lahko povzročijo osebne poškodbe, ki pa niso smrtne ali zelo hude.
- Varnostno opozorilo vas opozarja na stanja ali postopke, ki lahko povzročijo poškodbe na strojih, opremi ali programski opremi.

Referenčne številke v oklepajih, na primer (1), na koncu vsakega opozorila uporabite za uskladitev z želenim prevodom.

OPOZORILO:
Ta enota ima lahko dva priključka za omrežno napetost. Če želite v celoti odstraniti napajanje, izključite oba napajalna kabla. (1)



OPOZORILO:
V ZDA uporabljajte le enote GBIC ali izdelke z optičnimi vodniki, ki se skladajo s standardi FDA, 21 CFR podpoglavje J. Drugje po svetu uporabljajte le enote GBIC ali izdelke z optičnimi vodniki, ki se skladajo s standardom IEC 825-1. Optični izdelki, ki se ne skladajo s temi standardi, lahko oddajajo svetlobo, ki je škodljiva očem. (2)

SJ000338

OPOZORILO:
Litijeva baterija lahko povzroči požar, eksplozijo ali resne opekline. Zato je znova ne polnite, razstavite, segrevajte na temperature nad 100°C (212°F), prispajkajte neposredno na celico, sežgite ali izpostavljajte vsebine vodi. Hranite jo tako, da do nje ne bodo imeli dostopa otroci. Zamenjajte jo le s sestavnim delom, katerega številka je podana za vaš sistem. Uporaba druge baterije lahko povzroči požar ali eksplozijo. Spojnik baterije je polariziran; ne poskušajte zamenjati polaritete. Baterijo odvrzite v skladu z lokalnimi predpisi. (3)

SJSLV347

OPOZORILO:
Če baterije ne vstavite na pravilno mesto, lahko pride do eksplozije. Vse izrabljene baterije morate usmetiščiti v skladu z navodili proizvajalca.
Če ura dejanskega časa začne zaostajati, se obrnite na IBM. (4)

OPOZORILO:
Če ťelite odstraniti napajanje za model M12 računalnika 2109, izključite oba napajalna kabla. (5)

SJSLV699

Spanish

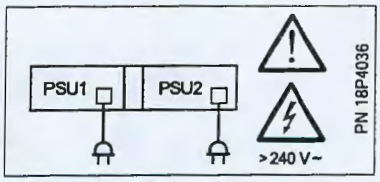
Avisos de seguridad

Los avisos de seguridad están impresos a lo largo de este manual.

- Un aviso de *Peligro* le avisa sobre condiciones o procedimientos que pueden causar la muerte o provocar daños personales graves.
- Un aviso de *Precaución* le avisa sobre condiciones o procedimientos que pueden causar daños personales que no provocan la muerte ni son muy peligrosos.
- Un aviso de *Atención* avisa sobre condiciones o procedimientos que pueden causar daños en máquinas, equipo o programas.

Utilice los nombres de referencia en paréntesis como, por ejemplo, (1) que se encuentran al final de cada aviso para saber cuál es la traducción deseada.

PRECAUCIÓN:
Esta unidad puede tener dos cables eléctricos. Para eliminar toda la alimentación, desconecte los dos cables. (1)



PRECAUCI N:
En los Estados Unidos utilice solamente unidades GBIC o productos de Fibra óptica que cumplan con los estándares de rendimiento de radiación de FDA, 21 CFR Subcapítulo J. A nivel internacional, utilice solamente unidades GBIC o productos de Fibra óptica que cumplan con el estándar 825-1 de IEC. Los productos ópticos que no cumplan dichos estándares pueden emitir luz perjudicial para la vista. (2)

SJ000338

PRECAUCIÓN:
Una batería de litio puede provocar incendios, explosiones o quemaduras graves. No se debe recargar, desmontar, calentar por encima de los 100 °C (212 °F), soldar directamente a la célula, incinerar ni exponer a humedades. Manténgase fuera del alcance de los niños. Sustituya solamente con el número de pieza especificado para su sistema. El utilizar otra batería puede implicar peligro de incendio o explosión. El conector de la batería está polarizado; no intente invertir la polaridad. Deseche la batería de acuerdo a las regulaciones locales. (3)

SJSPA347

PRECAUCIÓN:

Existe riesgo de explosión si la batería se sustituye de forma incorrecta. Todas las baterías usadas deben desecharse de acuerdo con las instrucciones del fabricante. Póngase en contacto con IBM si el reloj de tiempo real comienza a atrasarse. (4)

PRECAUCIÓN:
Para desconectar el conmutador 2109 Modelo M12 de la corriente eléctrica, desenchufe los dos cables de alimentación. (5)

SJSPA699

ROS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1421
Doc 3698

10439
A.

Swedish

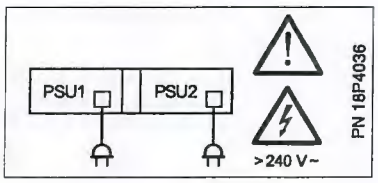
Säkerhetsinformation

Den här boken innehåller säkerhetsinformation.

- Meddelanden som föregås av ordet Fara varnar för tillstånd eller procedurer som kan orsaka död eller allvarlig personskada.
- Meddelanden som föregås av ordet Varning varnar för tillstånd eller procedurer som kan orsaka personskada som är vare sig dödlig eller extremt hälsovådlig.
- Meddelanden som föregås av ordet Obs varnar för tillstånd eller procedurer som kan orsaka skada på datorer, utrustning eller program.

Använd referensnumren inom parentes i slutet av varje meddelande, t ex (1), för en viss översättning.

VARNING:
Den här enheten kan ha två nätkablar. Koppla ur båda nätkablarna så att all ström bryts. (1)



VARNING:
I USA ska endast GBIC-enheter eller fiberoptiska produkter som uppfyller FDA-standarder för strålning, 21 CFR avsnitt J, användas. Internationellt ska endast GBIC-enheter eller fiberoptiska enheter som uppfyller IEC-standard 825-1 användas. Optiska produkter som inte uppfyller standarderna kan utstråla ljus som är skadligt för ögonen. **(2)**

SJ000338

VARNING:
Litiumbatterier kan orsaka brand, explosioner eller allvarliga brännskador. Batteriet får inte laddas om, hettas upp till mer än 100 grader celsius eller tas isär. Battericellen får inte lödas direkt på eller brännas, och dess innehåll får inte utsättas för vatten. Låt inte barn leka med batterierna. Ersätt bara med batterier med artikelnumret som gäller för det system du använder. Det kan innebära risk för eldsvåda eller explosion att använda ett batteri av annan typ. Försök aldrig kasta om batteriets poler. Följ lokala miljöföreskrifter när du slänger batteriet. (3)

SJSWE347

VARNING:
Det finns fara för explosion om batteriet byts ut på ett felaktigt sätt. Släng det använda batteriet i enlighet med tillverkarens anvisningar.
Kontakta IBM om klockan börjar gå långsammare. (4)

VARNING:
Bryt strömmen till 2109 modell M12 genom att koppla ur båda strömkablarna. (5)

SJSVE699

10438
A.

Notices

This information was developed for products and services offered in the U. S. A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504–1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1422
51
3698
Doc.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM
TotalStorage

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission statements

This section gives the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada compliance statement

Avis de conformite a la reglementation d'Industrie Canada: Cet appareil numerique de la classe A est conform a la norme NMB-003 du Canada.

Chinese Class A compliance statement

Attention: This is a Class A statement. In a domestic environment, this product might cause radio interference in which case the user might be required to take adequate measures.

10436
A-

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

European Community compliance statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product is in conformity with the EU council directive 73/23/EEC on the approximation of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits. This conformity is based on compliance with the following harmonized standard: EN60950.

This product has been tested and found to comply with the limits for class A Information Technology Equipment according to European Standard EN 55022. The limits for class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Where shielded or special cables (for example, cables fitted with ferrites) are used in the test to make the product comply with the limits:

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

Germany compliance statement

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische

Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG das

EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuellt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Notices 53
Fls Nº 1423
Doc: 3698

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:_|t¹|

"Geraete duerfen an Orten, fuer die sie nicht ausreichend entstoert sind, nur mit besonderer Genehmigung des Bundesministeriums fuer Post und Telekommunikation oder des Bundesamtes fuer Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Stoerungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs.4)

Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden

Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Nach der EN 55022:

"Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstoerungen verursachen. in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzufuehren und dafuer aufzukommen."

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen, sind die Geraete wie in den Handbuechern angegeben zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Government Ministry of Communication (MOC) statement

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this is not suitable for your use, you may exchange it for one with a non-business use.

Taiwan class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。 VS07171L

10434
A.

Glossary

This glossary provides definitions for the Fibre Channel and switch terminology used for the IBM 2109 Model M12. This glossary also provides definitions for the Fibre Channel and switch terminology used for the IBM TotalStorage SAN Cabinet 2109 Model C36.

This glossary defines technical terms and abbreviations used in this document. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at www.ibm.com/networking/nsg/nsgmain.htm

This glossary also includes terms and definitions from:

- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms*. New York: McGraw-Hill, 1994.

The following cross-reference conventions are used in this glossary:

See Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

See also Refers you to a related term.

8b/10b encoding. An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports

16-port card. The Fibre Channel port card provided with the 2109 Model M12. Contains 16 ports and the corresponding light-emitting diodes (LEDs). See also *port card.*

access control list (ACL). Enables an organization to bind a specific worldwide name (WWN) to a specific switch port or set of ports, preventing a port in another physical location from assuming the identity of a real WWN. Can also refer to a list of the read/write access of a particular community string. See also *device connection controls.*

account level switches. Switches that have four login accounts into the operating system (in descending order): root, factory, admin, and user. See also *admin account.*

ACL. See *access control list.*

address identifier. A 24-bit or 8-bit value used to identify the source or destination of a frame.

admin account. A login account intended for use by the customer to control switch operation. See also *account level switches.*

alias. An alternate name for an element or group of elements in the fabric. Aliases can be used to simplify the entry of port numbers and worldwide names (WWNs) when creating zones.

alias address identifier. An address identifier recognized by a port in addition to its standard identifier. An alias address identifier can be shared by multiple ports.

alias AL_PA. An arbitrated loop physical address (AL_PA) value recognized by a loop port (L_port) in addition to the AL_PA assigned to the port. See also *arbitrated loop physical address.*

alias server. A fabric software facility that supports multicast group management.

AL_PA. See *arbitrated loop physical address.*

American National Standards Institute (ANSI). The governing body for Fibre Channel standards in the U.S.A.

ANSI. See *American National Standards Institute.*

API. See *application programming interface.*

application programming interface (API). A defined protocol that allows applications to interface with a set of services.

application-specific integrated circuit (ASCI). In computer chip design, an integrated circuit created by first mounting an array of unconnected logic gates on a substrate and later connecting these gates in a particular configuration for a specific application. This design approach allows chips for a variety of applications to be made from the same generic gate array, thereby reducing production costs

ARB. See *arbitrate primitive signal.*

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1424
Doc. 3698

arbitrate primitive signal (ARB). A primitive signal that is transmitted as the fill word by a loop port (L_port) to indicate that the L_port is arbitrating to access to the loop. Applies only to the arbitrated loop topology.

arbitrated loop. A shared 100 MBps Fibre Channel transport structured as a loop and supporting up to 126 devices and one fabric attachment. A port must successfully arbitrate before a circuit can be established.

arbitrated loop physical address (AL_PA). An 8-bit value used to uniquely identify an individual port within a loop. A loop can have one or multiple AL_PAs.

arbitration wait timeout value (AW_TOV). The minimum time an arbitrating loop port (L_port) waits for a response before beginning loop initialization.

area number. A number that is assigned to each potential port location in the switch. Used to distinguish ports that have the same port number but are on different port cards.

ASIC. See *application-specific integrated circuit.*

asynchronous transfer mode (ATM). A broadband technology for transmitting data over local area networks (LANs) or wide area networks (WANs), based on relaying cells of fixed size. Provides any-to-any connectivity, and nodes can transmit simultaneously.

ATM. See *asynchronous transfer mode.*

auto-negotiate speed. Process that allows two devices at either end of a link segment to negotiate common features, speed (for example, 1 Gbps or 2 Gbps) and functions.

autoranging. A power supply that accommodates different input voltages and line frequencies.

autosense. Process during which a network device automatically senses the speed of another device.

AW_TOV. See *arbitration wait timeout value.*

backup FCS switch. The switch or switches assigned as backup in case the primary fabric configuration server (FCS) switch fails. See also *fabric configuration server switch* and *primary FCS switch.*

bandwidth. (1) The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). (2) The range of transmission frequencies available to a network. See also *throughput.*

basic input/output system (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BB_credit. See *buffer-to-buffer credit.*

beacon. When all the port light-emitting diodes (LEDs) on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by Telnet command or through Web Tools.

beginning running disparity. The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. See also *disparity.*

BER. See *bit error rate.*

BIOS. See *basic input/output system.*

BISR. Built-in self-repair.

bit error rate (BER). The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted. See also *error.*

blade. One component in a system that is designed to accept some number of components (blades). Blades could be individual servers that plug into a multiprocessing system or individual port cards that add connectivity to a switch. A blade is typically a hot swappable hardware device. See *16-port card.*

blind-mate connector. A two-way connector used in some switches to provide a connection between the system board and the power supply.

block. As applies to fibre channel, upper-level application data that is transferred in a single sequence.

bloom. Application-specific integrated circuit (ASIC) technology that the 2109 Model M12 is based on.

boot flash. Flash memory that stores the boot code and boot parameters. The processor runs its first instructions from boot flash. Data is cached in random access memory (RAM).

boot monitor. Code used to initialize the control processor (CP) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

British thermal unit (BTU). A measurement of heat produced in one hour.

broadcast. The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *multicast* and *unicast.*

BTU. See *British thermal unit.*

buffer-to-buffer credit. The number of frames that can be transmitted to a directly-connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. See also *buffer-to-buffer flow control.*

buffer-to-buffer flow control. Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. See also *buffer-to-buffer credit.*

CAM. Content addressable memory.

cascade. Two or more interconnected Fibre Channel switches that can build large fabrics. Switches can be cascaded up to 239 switches, with a recommended maximum of seven inter-switch links (no path longer than eight switches). See also *fabric* and *inter-switch link.*

central processing unit (CPU). A part of a computer that includes the circuits that control the interpretation and execution of instructions. A CPU in the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

chassis. The metal frame in which the switch and switch components are mounted.

circuit. An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions. See also *link.*

class 1. Service that provides a dedicated connection between two ports (also called connection-oriented service), with notification of delivery or nondelivery.

class 2. Connectionless service between ports with notification of delivery or nondelivery.

class 3. Connectionless service between ports without notification of delivery. Other than notification, the transmission and routing of class 3 frames is the same as class 2 frames.

class F. Connectionless service for inter-switch control traffic. Provides notification of delivery or nondelivery between two expansion ports (E_ports).

class of service. A specified set of delivery characteristics and attributes for frame delivery.

CLI. See *command line interface.*

CMI. Control message interface.

comma. A unique pattern (either 1100000 or 0011111) used in 8b/10b encoding to specify character alignment within a data stream. See also *K28.5.*

command line interface (CLI). Interface that depends entirely on the use of commands, such as through Telnet or simple network management protocol (SNMP), and does not involve a graphical user interface.

community (SNMP). A relationship between a simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

compact flash. Flash memory that stores the run-time operating system and is used like hard disk storage. Not visible within the memory space of the processor. Data is stored in file system format. Also called user flash.

control processor (CP). The central processing unit that provides all control and management functions in a switch.

control processor card (CP card). The central processing unit of the 2109 Model M12, which contains two control processor (CP) card slots to provide redundancy. Provides Ethernet, serial, and modem ports with the corresponding light-emitting diodes (LEDs).

core switch. A switch whose main task is to interconnect other switches. Also referred to as a backbone switch. See also *edge switch.*

CP. See *control processor.*

CP card. See *control processor card.*

CPLD. Complex programmable logic device.

CPU. See *central processing unit.*

CRC. See *cyclic redundancy check.*

credit. When applied to a switch, the maximum number of receive buffers provided by a fabric port (F_port) or fabric loop port (FL_port) to its attached node port (N_port) or node loop port (NL_port), respectively, such that the N_port or NL_port can transmit frames without over-running the F_port or FL_port.

CSA. Canadian Standards Association.

cut-through. A switching technique that allows the route for a frame to be selected as soon as the destination address is received. See also *route.*

cyclic redundancy check (CRC). A check for transmission errors included in every data frame.

data communications equipment (DCE) port. A port that is capable of interfacing between a data terminal equipment (DTE) port and a transmission circuit. DCE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *data terminal equipment (DTE) port.*

data rate. The rate at which data is transmitted or received from a device. Interactive applications tend to require a high data rate, while batch applications can usually tolerate lower data rates.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1425
Doc. 3698

data terminal equipment (DTE) port. A port that is capable of interfacing to a transmission circuit through a connection to a data communications equipment (DCE) port. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2 in a 9-pin connector (reversed in 25-pin connectors). See also *data communications equipment (DCE) port*.

DB-9 connector. A 9-pin version of the RS-232C port interface.

DCC. A dc converter.

DCE port. See *data communications equipment (DCE) port*.

DDR. Double data rate. See *data rate*.

defined zone configuration. The complete set of all zone objects that are defined in the fabric. The defined configuration can include multiple zone configurations. See also *enabled zone configuration* and *zone configuration*.

device. Hosts and storage that connect to a switch. Example devices are servers, redundant array of independent disks (RAID) arrays, and tape subsystems.

device connection controls. Enables organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by a worldwide name (WWN) and typically represent host bus adapters (HBAs) (servers). See also *access control lists*.

DID. The 3-byte destination ID of the destination device, in the 0xDomainAreaALPA format.

direct memory access (DMA). The transfer of data between memory and an input/output device without processor intervention.

disparity. The relationship of ones and zeros in an encoded character. *Neutral disparity* means an equal number of each, *positive disparity* means a majority of ones, and *negative disparity* means a majority of zeros.

DLS. See *dynamic load sharing*.

DMA. See *direct memory access*.

DNS. Distributed name server.

domain_ID. Unique identifier for the switch in a fabric. Usually automatically assigned by the switch, but can also be assigned manually. Can be any value between 1- 239.

DRAM. See *dynamic random access memory*.

DTE port. See *data terminal equipment (DTE) port*.

dual fabric. Two identical fabrics that allow redundancy in the event that one fabric fails. Use a dual fabric for mission critical applications.

dual-fabric SAN. A storage area network (SAN) that is composed of two independent fabrics. Synonymous with multi-fabric SAN. The two-fabric architecture makes dual-fabric SANs redundant.

DWDM. Dense wavelength digital multiplexing.

dynamic load sharing (DLS). Dynamic distribution of traffic over available paths. Allows for recomputing of routes when a fabric port or fabric loop port (Fx_port) or expansion port (E_port) changes status.

dynamic random access memory (DRAM). A storage in which the cells require repetitive application of control signals to retain stored data.

edge fabric. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric. See also *resilient core*.

edge switch. A switch whose main task is to connect nodes into the fabric. See also *core switch*.

E_D_TOV. See *error detect timeout value*.

EE_credit. See *end-to-end credit*.

effective zone configuration. The particular zone configuration that is currently in effect. Only one configuration can be in effect at once. The effective configuration is built each time a zone configuration is enabled.

EIA. Electronic Industry Association.

EIA rack. A storage rack that meets the standards set by the Electronics Industry Association (EIA).

electromagnetic compatibility (EMC). The design and test of products to meet legal and corporate specifications dealing with the emissions and susceptibility to frequencies in the radio spectrum. Electromagnetic compatibility is the ability of various electronic equipment to operate properly in the intended electromagnetic environment.

electromagnetic interference (EMI). Waves of electromagnetic radiation, including but not limited to radio frequencies, generated by the flow of electric current.

electrostatic discharge (ESD). The flow of current that results when objects having a static charge come into close enough proximity to discharge.

ELP. Extended link parameters.

ELWL. See *extra long wavelength*.

EMC. See *electromagnetic compatibility*.

EMI. See *electromagnetic interference*.

enabled zone configuration. The currently enabled configuration of zones. Only one configuration can be enabled at a time. See also *defined zone configuration* and *zone configuration.*

end port. A port on an edge switch that connects a device to the fabric.

end-to-end credit (EE_credit). The number of receive buffers allocated by a recipient port to an originating port. Used by class 1 and class 2 services to manage the exchange of frames across the fabric between source and destination. See also *end-to-end flow control* and *buffer-to-buffer credit.*

end-to-end flow control. Govems flow of class 1 and class 2 frames between node ports (N_ports). See also *end-to-end credit.*

E_port. See *expansion port.*

error. As applies to fibre channel, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors). See also *loop failure.*

error detect timeout value (E_D_TOV). The time that the switch waits for an expected response before declaring an error condition. Adjustable in 1 microsecond increments from 2 - 10 seconds.

ESD. See *electrostatic discharge.*

exchange. The highest level Fibre Channel mechanism used for communication between node ports (N_ports). Composed of one or more related sequences, and can work in either one or both directions.

expansion port (E_port). A port is designated an expansion port (E_port) when it is used as an inter-switch expansion port to connect to the E_port of another switch, to build a larger switch fabric.

Extended Fabrics. A feature that runs on Fabric operating system (OS) and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 km (62.14 mi).

extra long wavelength (ELWL). Laser light with a periodic length greater than 1300 nm (for example, 1420 or 1550). ELWL lasers are used to transmit Fibre Channel data over distances greater than 10 km. Also known as XLWL.

fabric. A network that uses high-speed fibre connections to connect switches, hosts, and devices. A fabric is an active, intelligent, nonshared interconnect scheme for nodes.

Fabric Access. Allows the application to control the fabric directly for functions such as discovery, access (zoning) management, performance, and switch control. Consists of a host-based library that interfaces the application to switches in the fabric over an out-of-band TCP/IP connection or in-band using an IP-capable host bus adapter (HBA).

Fabric Assist. A feature that enables private and public hosts to access public targets anywhere on the fabric, provided they are in the same Fabric Assist zone.

fabric configuration server (FCS) switch. One or more designated switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by worldwide name (WWN), and the list of designated switches is communicated fabric-wide. See also *backup FCS switch, primary FCS switch.*

fabric login (FLOGI). The process by which a device gains access to the fabric.

fabric loop port (FL_port). A fabric port that is loop capable. Used to connect node loop ports (NL_ports) to the switch in a loop configuration.

Fabric Manager. A feature that allows the storage area network (SAN) manager to monitor key fabric and switch elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values or counters and provides notification when defined boundaries are exceeded. The SAN manager can configure which elements, such as error, status, and performance counters, are monitored within a switch.

fabric mode. One of the modes for a loop port (L_port). An L_port is in fabric mode when it is connected to a port that is not loop capable and is using fabric protocol. See also *loop port* and *loop mode.*

fabric name. The unique identifier assigned to a fabric and communicated during login and port discovery.

Fabric OS. An operating system made up of two software components: the firmware that initializes and manages the switch hardware, and diagnostics.

fabric port (F_port). A port that is able to transmit under fabric protocol and interface over links. Can be used to connect a node port (N_port) to a switch. See also *fabric loop port* and *Fx_port.*

Fabric Watch. A feature that runs on Fabric operating system (OS) and allows monitoring and configuration of fabric and switch elements.

failover. The act that causes control to pass from one redundant unit to another.

FAN. Fabric address notification.

FC. See *fibre channel.*

FCA. See *Fibre Channel arbitrated loop.*

FC-AL. See *Fibre Channel arbitrated loop.*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1426
Nº 2 Doc. 3698

FC-AL-3. The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCC. Federal Communications Commission.

FC-FLA. The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCMGMT. Fibre Alliance Fibre Channel Management.

FCP. See *Fibre Channel protocol.*

FC-PDLA. The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FC-PH-1,2,3. The Fibre Channel Physical and Signaling Interface standards defined by ANSI.

FC-PI. The Fibre Channel Physical Interface standard defined by ANSI.

FCS switch. See *fabric configuration server switch.*

FC-SW-2. The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches in order to create a multiswitch Fibre Channel fabric.

Fibre Channel (FC). A technology for transmitting data between computer devices at a data rate of up to 4 Gbps. It is especially suited for attaching computer servers to shared storage devices and for interconnecting storage controllers and drives.

Fibre Channel arbitrated loop (FC-AL). A standard defined on top of the FC-PH standard. It defines the arbitration on a loop where several FC nodes share a common medium.

Fibre Channel protocol (FCP). The protocol for transmitting commands, data, and status using Fibre Channel FC-FS exchanges and information units. Fibre channel is a high-speed serial architecture that allows either optical or electrical connections at data rates from 265 Mbps up to 4-Gbps.

Fibre Channel service (FS). A service that is defined by Fibre Channel standards and exists at a well-known address. For example, the Simple Name Server is a Fibre Channel service. See also *Fibre Channel service protocol.*

Fibre Channel service protocol (FSP). The common protocol for all fabric services, transparent to the fabric type or topology. See also *Fibre Channel service.*

Fibre Channel shortest path first (FSPF). A routing protocol used by Fibre Channel switches.

Fibre Channel transport. A protocol service that supports communication between Fibre Channel service providers. See also *Fibre Channel service protocol.*

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit can contain other field replaceable units.

File Transfer protocol (FTP). In Transmission Control protocol/Internet protocol (TCP/IP), an application protocol used for transferring files to and from host computers.

fill word. An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

firmware. The basic operating system provided with the hardware.

FLA. Fabric loop attach.

flash partition. Two redundant usable areas, called *partitions* into which firmware can be downloaded in the 2109 Model M12.

FLOGI. See *fabric login.*

FL_port. See *fabric loop port.*

F_port. See *fabric port.*

frame. The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, the data payload, a cyclic redundancy check (CRC), and an end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements, and so on) and data frames.

frame delimiter. A part of an ordered set that marks frame boundaries and describes frame contents. See also *ordered set.*

FRU. See *field replaceable unit.*

FS. See *Fibre Channel service.*

FSP. See *Fibre Channel service protocol.*

FSPF. See *Fibre Channel shortest path first.*

FTP. See *File Transfer protocol.*

full duplex. A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *half duplex.*

Fx_port. A fabric port that can operate as either a fabric port (F_port) or fabric loop port (FL_port). See also *fabric port* and *fabric loop port.*

gateway. Hardware that connects incompatible networks by providing the necessary translation for both hardware and software.

GBIC. See *gigabit interface converter.*

Gbps. Gigabits per second.

GBps. Gigabytes per second.

generic port (G_port). A generic port that can operate as either an expansion port (E_port) or a fabric port (F_port). A port is defined as a G_port when it is not yet connected or has not yet assumed a specific function in the fabric.

gigabit interface converter (GBIC). A removable serial transceiver module designed to provide gigabaud capability for fibre channel (FC) and other products that use the same physical layer.

gigabit switch. A 16-port, Fibre Channel gigabit switch.

G_port. See *generic port.*

half duplex. A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time). See also *full duplex.*

hard address. The arbitrated loop physical address (AL_PA) that a node loop port (NL_port) attempts to acquire during loop initialization.

hardware translative mode. Method for achieving address translation. The two hardware translative modes that are available to a QuickLoop-enabled switch are standard translative mode and QuickLoop mode. See also *standard translative mode* and *QuickLoop mode.*

HBA. See *host bus adapter.*

heartbeat. Through clustering software, the application server continually communicates with the clustered spare using network heartbeats to indicate to the other machines that everything is operating correctly. This heartbeat is typically carried over a dedicated network for clustering traffic. In cases of a problem (for example, a software crash on the operational server or a hardware component failure), a heartbeat link indicates to the other server that something has failed or is otherwise inoperative. If that heartbeat is lost, the spare server takes over the function provided by the application service. Depending on the clustering software, either the entire server or only specific services on the server can be failed over or failed back.

high availability. An attribute of the switch that identifies it as being capable of operating well in excess of 99 percent of the time. High availability is typically identified by the number of nines in that percentage. For example, a switch that is rated at five nines would be capable of operating 99.999 percent of the time without failure.

high port count fabric. A fabric containing 100 or more ports.

host bus adapter (HBA). The interface card between a server or workstation bus and the Fibre Channel network.

hot pluggable. A field replaceable unit (FRU) capability that indicates it can be extracted or installed while customer data is otherwise flowing in the chassis.

hub. A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

IC bus. A serial, 2-wire bus used to monitor field replaceable unit (FRU) temperatures and control the system including blade power control.

ID. Identification.

IDB. Interface descriptor block.

IDLE. Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

IEC. International Electrotechnical Commission.

IETF. Internet Engineering Task Force.

information unit (IU). A set of information as defined by either upper-level process protocol definition or upper-lever protocol mapping.

initiator. A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *target.*

in-order delivery (IOD). A parameter that, when set, guarantees that frames are either delivered in order or dropped.

integrated fabric. The fabric created by six switches cabled together and configured to handle traffic as a seamless group.

Internet protocol (IP). In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

inter-switch link (ISL). A Fibre Channel link that connects two switches (a link from the expansion port (E_port) of one switch to the E_port of another).

10428
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1427
Doc. 3698

IOD. See *in-order delivery.*

IP. See *internet protocol.*

IPA. Initial process associator.

ISL. See *inter-switch link.*

ISL Trunking. A feature that enables distribution of traffic over the combined bandwidth of up to four inter-switch links (ISLs) (between adjacent switches), while preserving in-order delivery. A set of trunked ISLs is called a trunking group; each port employed in a trunking group is called a trunking port. See also *master port.*

isolated E_port. An expansion port (E_port) that is online but not operational between switches due to overlapping domain ID or nonidentical parameters such as error delay timeout values (E_D_TOVs). See also *expansion port.*

IU. See *information unit.*

K28.5. A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern. See also *comma.*

kernel flash. Flash memory that stores the bootable kernel code and is visible within the memory space of the processor. Data is stored as raw bits.

key pair. In public key cryptography, a pair of keys consisting of a public and private key of an entity. The public key can be publicized, but the private key must be kept secret.

LAN. See *local area network.*

latency. The period of time required to transmit a frame, from the time it is sent until it arrives.

LED. See *light-emitting diode.*

light-emitting diode (LED). A semiconductor chip that gives off visible or infrared light when activated.

link. As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibers. See also *circuit.*

link services. A protocol for link-related services.

LIP. See *loop initialization primitive.*

LM_TOV. See *loop master timeout value.*

local area network (LAN). A computer network located on a user's premises within a limited geographical area. (T)

logical unit number (LUN). An identifier used on a small computer systems interface (SCSI) bus to distinguish among up to eight devices (logical units) with the same SCSI ID.

long wavelength (LWL). A type of fiber optic cabling that is based on 1300 mm lasers and supports link speeds of 1.0625 Gbps. Can also refer to the type of GBIC or SFP. See also *short wavelength.*

loop. A configuration of devices that are connected to the fabric by way of a fabric loop port (FL_port) interface card.

loop circuit. A temporary bidirectional communication path established between loop ports (L_ports).

loop failure. Loss of signal within a loop for any period of time, or loss of synchronization for longer than the timeout value.

loop_ID. A hexadecimal value representing one of the 127 possible arbitrated loop physical address (AL_PA) values in an arbitrated loop.

loop initialization. The logical procedure used by a loop port (L_port) to discover its environment. Can be used to assign arbitrated loop physical address (AL_PA) addresses, detect loop failure, or reset a node.

loop initialization primitive (LIP). The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

looplet. A set of devices connected in a loop to a port that is a member of another loop.

loop master timeout value (LM_TOV). The minimum time that the loop master waits for a loop initialization sequence to return.

loop mode. One of the modes for a loop port (L_port). An L_port is in loop mode when it is in an arbitrated loop and is using loop protocol. An L_port in loop mode can also be in participating mode or nonparticipating mode. See also *loop port*, *fabric mode*, *participating mode*, and *nonparticipating mode.*

loop port (L_port). A node port (NL_port) or fabric port (FL_port) that has arbitrated loop capabilities. An L_port can be either in fabric mode or loop mode. See also *fabric mode* , *loop mode, nonparticipating mode,* and *participating mode.*

loop port state machine (LPSM). The logical entity that performs arbitrated loop protocols and defines the behavior of loop ports (L_ports) when they require access to an arbitrated loop.

L_port. See *loop port.*

LPSM. See *loop port state machine.*

LSR. Link state record.

10426

LSU. Link state update.

LUN. See *logical unit number.*

LWL. See *long wavelength.*

MAC. Media access controller.

management information base (MIB). A simple network management protocol (SNMP) structure to help with device management, providing configuration and device information.

master port. As relates to trunking, the port that determines the routing paths for all traffic flowing through the trunking group. One of the ports in the first inter-switch link (ISL) in the trunking group is designated as the master port for that group. See also *ISL Trunking.*

MIB. See *management information base.*

modem serial port. The upper serial port on the control processor card (CP card) of the 2109 Model M12. Can be used to connect the CP card to a modem with a standard 9-pin modem cable. Consists of a DB-9 connector wired as an RS-232 device, and can be connected by serial cable to a data communications equipment (DCE) device. A Hayes-compatible modem or Hayes-emulation is required. The device name is ttyS1. See also *data communications equipment port* and *terminal serial port.*

multicast. The transmission of data from a single source to multiple specified node ports (N_ports), as opposed to all the ports on the network. See also *broadcast* and *unicast.*

multimode. A fiber optic cabling specification that allows up to 500 m (1640.5 ft) between devices.

name server. Frequently used to indicate Simple Name Server. See also *simple name server.*

NEMA. National Electrical Manufacturers Association.

NL_port. See *node loop port.*

NMS. Network Management System.

node. A Fibre Channel device that contains a node port (N_port) or node loop port (NL_port).

node loop port (NL_port). A node port that is loop capable. Used to connect an equipment port to the fabric in a loop configuration through a fabric loop port (FL_port).

node name. The unique identifier for a node, communicated during login and port discovery.

node port (N_port). A node port that is not loop capable. Used to connect an equipment port to the fabric.

nonparticipating mode. A mode in which a loop port (L_port) in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an arbitrated loop physical address (AL_PA) cannot be acquired. See also *participating mode.*

nonvolatile random access memory (NVRAM). Random access memory (storage) that retains its contents after the electrical power to the machine is shut off. A specific part of NVRAM is set aside for use by the system ROS for the boot device list.

N_port. See *node port.*

NVRAM. See *nonvolatile random access memory.*

Nx_port. A node port that can operate as either a node port (N_port) or node loop port (NL_port). See also *node port* and *node loop port.*

operating system (OS). A collection of system programs that control the overall operation of a computer system.

ordered set. A transmission word that uses 8b/10b mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include frame delimiters, primitive signals, and primitive sequences. Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames. See also *frame delimiter, primitive signal,* and *primitive sequence.*

OS. See *operating system.*

packet. A set of information transmitted across a network. See also *frame.*

participating mode. A mode in which a loop port (L_port) in a loop has a valid arbitrated loop physical address (AL_PA) and can arbitrate, send frames, and retransmit received transmissions. See also *nonparticipating mode.*

path selection. The selection of a transmission path through the fabric. Switches use the Fibre Channel shortest path first (FSPF) protocol.

PCI. Peripheral control interconnect.

PDU. Power distribution unit.

Performance Monitoring. A feature that provides error and performance information to the administrator and user for use in storage management.

phantom address. An arbitrated loop physical address (AL_PA) value that is assigned to a device that is not physically in the loop. Also known as phantom AL_PA.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1428
Doc. 3698

phantom device. A device that is not physically in an arbitrated loop, but is logically included through the use of a phantom address.

PLDA. See *private loop direct attach.*

PLOGI. See *port login.*

PMC. PCI mezzanine card.

P/N. Part number.

point-to-point. A Fibre Channel topology that employs direct links between each pair of communicating entities.

port cage. The metal casing extending out of the optical port on the switch, and in which the gigabit interface converter (GBIC) or small form-factor pluggable (SFP) can be inserted.

port card. A Fibre Channel card that contains optical or copper port interfaces, and acts like a switch module. See also *16-port card.*

port login (PLOGI). The port-to-port login process by which initiators establish sessions with targets. See also *fabric login.*

port module. A collection of ports in a switch.

port_name. The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST. See *power-on self-test.*

power-on self-test (POST). A series of diagnostics that are automatically run by a device when the power is turned on.

primary FCS switch. Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric. See also *backup FCS switch* and *FCS switch.*

primitive sequence. A part of an ordered set that indicates or initiates port states. See also *ordered set.*

primitive signal. A part of an ordered set that indicates events. See also *ordered set.*

principal switch. The switch that assumes the responsibility to assign domain IDs. The role of principal switch is negotiated after a "build fabric" event.

private device. A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.

private loop. An arbitrated loop that does not include a participating fabric loop port (FL_port).

private loop direct attach (PLDA). A subset of fibre channel standards for the operation of peripheral devices.

private NL_port. A node loop port (NL_port) that communicates only with other private NL_ports in the same loop and does not log into the fabric.

protocol. A defined method and a set of standards for communication.

public device. A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

public loop. An arbitrated loop that includes a participating fabric loop port (FL_port), and can contain both public and private node loop ports (NL_ports).

public NL_port. A node loop port (NL_port) that logs into the fabric, can function within either a public or private loop, and can communicate with either private or public NL_ports.

quad. A group of four adjacent ports that share a common pool of frame buffers.

QuickLoop. (1) A feature that makes it possible to allow private devices within loops to communicate with public and private devices across the fabric through the creation of a larger loop. (2) The arbitrated loop created using this software. A QuickLoop can contain a number of devices or looplets; all devices in the same QuickLoop share a single arbitrated loop physical address (AL_PA) space.

QuickLoop mode. A hardware translative mode that allows private devices to communicate with other private devices across the fabric. See also *hardware translative mode* and *standard translative mode.*

RAID. See *redundant array of independent disks.*

RAM. See *random access memory.*

RAN. Remote Asynchronous Notification.

random access memory (RAM). A temporary storage location in which the central processing unit (CPU) stores and executes its processes.

R_A_TOV. See *resource allocation timeout value.*

read only memory (ROM). Memory in which stored data cannot be changed by the user except under special conditions.

receiver ready (R_RDY). A primitive signal indicating that the port is ready to receive a frame.

reduced instruction set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid processing.

redundant array of independent disks (RAID). A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

registered state change notification (RSCN). A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

remote fabric. A fabric that spans across wide area networks (WANs) by using protocol translation (a process also known as tunneling) such as fibre channel over asynchronous transfer mode (ATM) or fibre channel over Internet protocol (IP).

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server.

Remote Switch. A feature that runs on Fabric operating system (OS) and enables two fabric switches to be connected over an asynchronous transfer mode (ATM) connection. This requires a compatible Fibre Channel to ATM gateway, and can have a distance of up to 10 km (6.214 mi) between each switch and the respective ATM gateway.

request rate. The rate at which requests arrive at a servicing entity. See also *service rate.*

resilient core. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric.

resource allocation timeout value (R_A_TOV). Used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. This value is adjustable in one microsecond increments from 10 - 120 seconds.

resource recover timeout value (RR_TOV). The minimum time a target device in a loop waits after a loop initialization primitive (LIP) before logging out a small computer systems interface (SCSI) initiator. See also *error detect timeout value* and *resource allocation timeout value.*

RISC. See *reduced instruction set computer.*

RLS probing. Read link status of the arbitrated loop physical addresses (AL_PAs).

RPC. See *remote procedure call.*

10424
A.

R_RDY. See *receiver ready.*

RR_TOV. See *resource recovery timeout value.*

RS-232 port. A port that conforms to a set of Electrical Industries Association (EIA) standards. Used to connect data terminal equipment (DTE) and data communications equipment (DCE) devices for communication between components, terminals, and modems. See also *DB-9 connector, DCE port,* and *DTE port.*

RSCN. See *registered state change notification.*

RSH. Remote shell.

RTC. Real time clock.

rw. Read-write.

SAN. See *storage area network.*

SAN island. A group of storage devices and servers connected to switches in a fabric.

SC. Standard connector.

SCSI. See *small computer systems interface.*

SCSI Enclosure Services (SES). A subset of the small computer systems interface (SCSI) protocol used to monitor temperature, power, and fan status for enclosure devices.

SDRAM. See *synchronous dynamic random access memory.*

Secure Fabric OS. An optionally-licensed software product that runs on top of the Fabric OS and provides customizable security restrictions through local and remote management channels on a switch.

secure sockets layer (SSL). A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

sequence. A group of related frames transmitted in the same direction between two node ports (N_ports).

---

ro. Read only.

ROM. See *read only memory.*

route. As applies to a fabric, the communication path between two switches. Can also apply to the specific path taken by an individual frame, from source to destination. See also *Fibre Channel shortest path first.*

routing. The assignment of frames to specific switch ports, according to frame destination.

SERDES. Serializer/deserializer.

service rate. The rate at which an entity can service requests. See also *request rate.*

SES. See *SCSI Enclosure Services.*

SFP. See *small form-factor pluggable.*

short wavelength (SWL). A type of fiber optic cabling that is based on 850 mm lasers and supports 1.0625 Gbps link speeds. Can also refer to the type of gigabit

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1429
3698
Doc.

interface converter (GBIC) or small form-factor pluggable (SFP). See also *long wavelength*.

SID. The 3-byte source ID of the originator device, in the 0xDomainAreaALPA format.

SID-DID. Source identifier-destination identifier.

SIMMS. Single in-line modules.

simple name server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Can also be referred to as directory service. See also *Fibre Channel service*.

simple network management protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

single mode. The fiber optic cabling standard that corresponds to distances of up to 10 km (6.214 mi) between devices.

small computer systems interface (SCSI). A parallel bus architecture and a protocol for transmitting large data blocks up to a distance of 15 - 25 m (49 - 82 ft).

small form-factor pluggable (SFP). An optical transceiver used to convert signals between optical fiber cables and switches.

SMI. Special memory interface.

SNIA. Storage Network Industry Association.

SNMP. See *simple network management protocol*.

SNMPv1. The original standard for SNMP, now labeled v1.

SNS. See *simple name server*.

SOF. Start-of-frame.

SSL. See *secure sockets layer*.

standard translative mode. A hardware translative mode that allows public devices to communicate with private devices across the fabric. See also *hardware translative mode* and *QuickLoop mode*.

storage area network (SAN). A network of systems and storage devices that communicate using Fibre Channel protocols. See also *fabric*.

subordinate switch. All switches in the fabric other than the principal switch. See also *principal switch*.

switch. Hardware that routes frames according to Fibre Channel protocol and is controlled by software.

switch name. The arbitrary name assigned to a switch.

switch port. A port on a switch. Switch ports can be expansion ports (E_ports), fabric ports (F_ports), or fabric loop ports (FL_ports).

SWL. See *short wavelength*.

synchronous dynamic random access memory (SDRAM). The main memory for the switch. Used for volatile storage during switch operation.

Tachyon. A type of host bus adapter.

target. A storage device on a Fibre Channel network. See also *initiator*.

TCP. See *transmission control protocol*.

tenancy. The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

terminal serial port. The lower serial port on the control processor card (CP card) of the 2109 Model M12. This port sends switch information messages and can receive commands. Can be used to connect the CP card to a computer terminal. Has an RS-232 connector wired as a data terminal equipment (DTE) device, and can be connected by serial cable to a data communications equipment (DCE) device. The connector pins 2 and 3 are swapped so that a straight-through cable can be used to connect to a terminal. The device name is ttyS0. Can also be referred to as the console port. See also *DCE port, DTE port,* and *modem serial port*.

throughput. The rate of data flow achieved within a cable, link, or system. Usually measured in bits per second (bps). See also *bandwidth*.

topology. As applies to fibre channel, the configuration of the Fibre Channel network and the resulting communication paths allowed.

translative mode. A mode in which private devices can communicate with public devices across the fabric.

transmission character. A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Control protocol (TCP). A communications protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for Internet protocol.

transmission word. A group of four transmission characters.

10422
A.

trap (SNMP). The message sent by a simple network management protocol (SNMP) agent to inform the SNMP management station of a critical error. See also *simple network management protocol.*

tunneling. A technique for enabling two networks to treat a transport network as though it were a single communication link or local area network (LAN).

Tx. Transmitted.

U. Unit of measure for rack-mounted equipment.

UART. Universal Asynchronous Receiver Transmitter.

UDP. See *user datagram protocol.*

ULP. See *upper-level protocol.*

ULP_TOV. See *upper-level timeout value.*

unicast. The transmission of data from a single source to a single destination. See also *broadcast* and *multicast.*

universal port (U_port). A switch port that can operate as a generic port (G_port), expansion port (E_port), fabric port (F_port), or fabric loop port (FL_port). A port is defined as a U_port when it is not connected or has not yet assumed a specific function in the fabric.

U_port. See *universal port.*

upper-level protocol (ULP). The protocol that runs on top of Fibre Channel. Typical upper-level protocols are small computer system interface (SCSI), Internet protocol (IP), HIPPI, and IPI.

upper-level timeout value (ULP_TOV). The minimum time that a small computer system interface (SCSI) upper-level protocol (ULP) process waits for SCSI status before initiating ULP recovery.

user datagram protocol (UDP). A protocol that runs on top of Internet protocol (IP) and provides port multiplexing for upper-level protocols.

user flash. See *compact flash.*

VC. See *virtual circuit.*

VCCI. Voluntary Control Council for Interference

virtual circuit (VC). A one-way path between node ports (N_ports) that allows fractional bandwidth.

WAN. See *wide area network.*

WDM. Wave division multiplexing.

well-known address. As pertaining to fibre channel, a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan network, and that can use or provide public communications facilities. (T)

workstation. A computer used to access and manage the fabric. Can also be referred to as a management station or host.

worldwide name (WWN). Uniquely identifies a switch on local and global networks.

World Wide Web (WWW). A network of servers that contain programs and files. Many of the files contain hypertext links to other documents available through the network.

WWN. See *worldwide name.*

WWW. See *World Wide Web.*

XLWL. See *extra long wavelength.*

zone. A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone. See also *zoning.*

zone alias. An alias for a set of port numbers or worldwide names (WWNs). Zone aliases can be used to simplify the entry of port numbers and WWNs. For example, "host" could be used as an alias for a WWN of 110:00:00:60:69:00:00:8a.

zone configuration. A set of zones designated as belonging to the same zone configuration. When a zone configuration is in effect, all valid zones in that configuration are also in effect.

zone member. A port, node, worldwide name (WWN), or alias, which is part of a zone.

zone scheme. The level of zoning granularity selected. For example, zoning can be done by switch or port, worldwide name (WWN), arbitrated loop physical address (AL_PA), or a mixture. See also *zone configuration.*

zone set. See *zone configuration.*

Zoning. A feature that runs on Fabric operating system (OS) and allows partitioning of the fabric into logical groupings of devices. Devices in a zone can only access and be accessed by devices in the same zone. See also *zone.*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1430
Nº 3698
Doc.

10421
A.

Index

Numerics

16-port card specifications 18
2109 Model C36 with Model M12 library xv
2N power architecture 8

A

about this document
  related publications xv
  who should read this document xv
ac input 8
address
  director of licensing 51
  IBM xvii
Advanced Security feature 13

B

battery notice xiv
battery specifications 19
Brocade
  documents xv
  IBM product and model number matrix xvi

C

cable
  management 7
  side, LEDs 12
caution notices
  battery xiv
  customer setup xi
  example xi
  laser safety xiii
  linecord xii
  translations 27
certification, safety 25
checking safety labels xi
Chinese Class A compliance statement 52
Class 1 laser product xiii
comments, how to send xvii
compliance, regulatory 25
components
  switch 17
  weight 17
configuration, CP blade assembly 10
cooling system 6
CP blade assembly
  configuration 10
  description 9
  management 10
CPU subsystem 9
customer setup caution notice xi

D

danger notices
  electrical outlet xi
  example xi
  translations 27
dc outputs 8
design
  high availability 4
  overview 3
  switch blade assembly 11
diagnostic tests 12
dimensions of the switch 17
director of licensing, address 51
disposal, product xiv

E

electronic emission statements 52
EMC (electromagnetic compatibility) 25
EMI (electromagnetic interference) 25
environmental
  notices xiii
  requirements 22
Ethernet ports 5
European Community compliance statement 53
Extended Fabrics 13

F

Fabric Manager 14
Fabric OS
  description 14
facility specifications 20
fault monitoring and diagnostics 12
FCC
  emission limits 52
  rules 52
  statement 52
FDA 21 CFR 1040.10 and 1040.11 xiii
features
  Advanced Zoning 14
  Fabric Watch 14
  ISL Trunking 14
  Performance Monitoring 14
  software 13
    Advanced Security 13
    Extended Fabrics 13
    Fabric Manager 14
    Fabric OS 13
    Remote Switch 13
  Web Tools 14
Federal Communications Commission (FCC)
 statement 52
Fibre Channel Association Web site xvi
field replaceable units 16
fire suppression systems xiv

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1431
3698
Doc.

form
reader comment, how to send xvii
FRUs (field replaceable units) 16

G

GBIC label on the 2109 Model M12 xi
general specifications of the switch 22
Germany compliance statement 53
getting
help xvi
software updates xvi

H

help, getting xvi
high availability design 4
how to send your comments xvii

I

IBM
address xvii
director of licensing, address 51
trademarks 52
IBM product and model number matrix xvi
IEC 825-1 xiii
immunity 26
indicators, system status 12
Industry Canada compliance statement 52
intellectual property 51
interference, radios and televisions 52
interoperability, description 15
introduction 1

J

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 54

K

Korean Government Ministry of Communication (MOC) statement 54

L

label
check, safety xi
laser safety caution xii, xiii
linecord caution xii
safety xiii
SFP xii
laser safety xiii
LEDs
cable-side 12
card 7
noncable side 13
license for patents 51
linecord caution label xii, xiii
link distance, high-speed Fibre Channel switch 2

M

management
cable 7
CP blade assembly 10
materials, recyclable xiv
memory specifications 19
modem serial port specifications 20

N

network manageability 15
noncable side LEDs 13
notices
caution, battery xiv
edition ii
environmental xi, xiii
example of caution xi
example of danger xi
IBM 51
safety xi
safety translation xi
numbering 6

O

optical port
description 5
terminators xiii
overview
product 1
system design 3

P

patents 51
port
description 5
Ethernet 5
optical 5
serial 6
switch 17
power distribution system
specifications 7
strategy 8
power specifications of the switch 21
product
disposal xiv
overview 1
recycling xiv
specifications 18
publications
2109 Model C36 with Model M12 library xv
Web sites xvi

R

rack mounting 6
radio interference 52
reader comment form processing xvii
recycling products xiv
regulatory
  compliance 25
  specifications 23
related documents xv
reliability 4
Remote Switch 13
requirements, environmental 22
restrictions, usage xiii

S

safety
  certifications 25
  label xi
  label checks xi
  laser xi, xiii
  notice translations xi
  notices xi
  product disposal xiv
security, description 15
sending your comments xvii
serial ports 6
serviceability 5
SFP
  description 2
  label xii
small form factor pluggable optical fiber optic transceivers 2
software
  features 13
    Advanced Security 13
    Advanced Zoning 14
    Extended Fabrics 13
    Fabric Manager 14
    Fabric OS 13
    Fabric Watch 14
    ISL Trunking 14
    Performance Monitoring 14
    Remote Switch 13
    Web Tools 14
  getting updates xvi
specifications
  16-port card 18
  battery 19
  facility 20
  general 22
  memory 19
  modem serial port 20
  power 21
  product 18
  regulatory 23
  terminal serial port 19
statements
  Chinese Class A compliance 52
  electronic emission 52
statements *(continued)*
  European Community compliance 53
  Federal Communications Commission 52
  Germany compliance 53
  Industry Canada compliance 52
  Japanese Voluntary Control Council for Interference (VCCI) class 1 54
  Korean Government Ministry of Communication (MOC) 54
  Taiwan class A compliance 54
strategies, power distribution 8
subsystem, CPU 9
switch
  components 17
  dimensions 17
  overview 1
  ports 17
  specifications
    facility 20
    general 22
    memory 19
    modem serial port 20
    power 21
    regulatory 23
    terminal serial port 19
  weight 17
switch blade assembly
  description 11
  design 11
system
  cooling 6
  design, overview 3
  fabric operating 14
  fire suppression xiv
  power distribution 7
  status indicators 12

T

Taiwan class A compliance statement 54
take-back program, product xiv
terminal serial port specifications 19
terminators for optical ports xiii
tests, diagnostic 12
throughput, high-speed Fibre Channel switch 2
trademarks 52
transceivers, SFP 2
translations, danger and caution notices 27

U

unauthorized changes or modifications 52
updates, getting software xvi
usage restrictions xiii

V

voltage label xiii

10419
A.

RQS nº 03/2005 - CN
CPMI
Fls Nº 1432
3698
Doc.

W

Web sites xvi
weight of the switch and components 17
who should read this document xv

Readers' comments — we would like to hear from you.

10417
A.

IBM TotalStorage SAN Switch
2109 Model M12 User's Guide

Publication No. GC26-7468-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1438
Doc: 3698

Readers' Comments — We'd Like to Hear from You
GC26-7468-02

IBM®

Cut or F
Along Li

10416
A.

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
RCF Processing Department
Dept. M86/Bldg.050-3
5600 Cottle Road
San Jose, CA
U.S.A. 95193-0001

Fold and Tape | **Please do not staple** | Fold and Tape

GC26-7468-02

Cut or Fold
Along Line

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1434
Nº 3698
Doc.

Spine information:

IBM

IBM TotalStorage SAN Switch 2109 Model M12 User's Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1435
3698
Doc.

Itautec

10413
A.

ANEXO 3

CATÁLOGOS, MANUAIS E OUTROS DOCUMENTOS TÉCNICOS

VOLUME 2

CONTEÚDO:

MANUAL 8

MANUAL 9

MANUAL 10

SCS Q. 01 Bloco "F" 11º Andar – Ed. Camargo Corrêa – Brasília-DF CEP: 70397-900 - Fone: (61) 323-3031 Fax: (61) 226-1251

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1436
Nº 3698
Doc.

1041 R
A.

Manual 08

3583 Ultrium Scalable Tape Library

Interoperability Matrix

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1437
3698
Doc

3583 Ultrium Scalable Tape Library

1041
A

Interoperability Matrix (List of Supported Servers)

Last Update Date: 5/06/03

Midrange and Open Systems Connectivity

IBM's TotalStorage Ultrium Scalable Tape Library 3583 provides a single storage solution designed to provide superior performance for many hardware and software systems.

Supported Independent Software (ISV) Vendors
Get the latest firmware and device drivers.

Supported Servers

Hewlett-Packard Servers
IBM iSeries and AS/400 Servers
IBM pSeries, RS/6000 and SP Servers
Microsoft Windows Servers
SUN Servers
Linux Support

Open Systems Support

The supported open systems environments are shown below. The sales representative and/or customer responsible for insuring that the specific host system configuration used (i.e. server model, operating system level and host adapter combination) is a valid and supported configuration.

Note:
IBM development plans are subject to change or withdrawal at any time without prior notice.

Hewlett-Packard Servers

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
HP 9000 Series	**HP-UX**	**HP**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1438
Doc 3698

A (rp2400), L (rp5400), N (rp7400) Class L, N Class	11.0 11.i	HP4800A (PCI)HVD Ultra; HP5149A (PCI) LVD Ultra2; HP5150A (PCI) LVD Ultra2

Notes

1. For V Class Servers, adapter 4800A requries the inline HVD SCSI terminator, Feature 5098.
2. The 3rd edition (E1298) of the HP Service and User's Guide for the 4800A PCI Ultra SCSI HBA specifies support for HP V22xx and V25xx Servers. Support for V2600 is not documented although the V2500/V2600 System Upgrade Guide (1st Edition) does not mention any adapter incompatibilities.
3. The 5150A PCI to Ultra 2 SCSI HBA Service and User Guide (2nd Edition, 2001) does not indicate support for V Class Systems - only N and L Class.
4. The 5149A PCI to Ultra 2 SCSI HBA Service and User Guide (2nd Edition, 2001) indicates support for V Class systems including the V2600 under HP-UX 11.0 and 11i. For V Class systems attach, HP specifies the 5M V-Class SE/LVD inline termination cable.

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models

Servers	Operating Systems	Host Adapters/SAN
HP 9000 Series	**HP-UX**	**HP**
A (rp2400), L (rp5400), N (rp7400) Class L, N Class	11.0 patch PHKL 21834 for N-Class; patch PHKL 22903 for L-Class 11.i	Click Here for details.

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultium Scalable Tape Library
2. For Details and guidelines click here.

IBM @server iSeries and AS/400 Servers

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models

Servers	Operating Systems	Host Adapters
Servers that support the listed host adapters.	**OS/400** V5R1, V5R2	FC 6501[1] HVD (Ultrium 1 Only); FC 6534 HVD; FC 2729 HVD Ultra PCI; FC 2749 HVD Ultra PCI; FC 5702 LVD Ultra PCI [2] (Ultrium 2 Only)

Notes

(1) Interposer for AS/400 Feature # 6501(Feature code 2895 on the 3583 Ultrium Tape Library)
(2) Requires V5R2

(3) For D-mode IPL, the device SCSI address must be set tp "0"

(4) One iSeries host and one device per SCSI 3583

10409

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters/SAN**
Servers that support the listed host adapters.	**OS/400** V5R1, V5R2	Click here for details.

Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.
2. The iSeries Fibre Channel attach supports multiple hosts and maximum six drive configurations for the 3583 Feature 8005 device.
3. D-mode IPL is not supported with Fibre Channel attached tape drives. The Alternate Installation Device (Boot Manager) support must be used.

   Note: You will need to order the appropriate feature(s) to your 3583 Ultrium Scalable Tape Library.

IBM @server pSeries and RS/6000 and RS/6000 SP Servers

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
Servers that support the listed host adapters.	**AIX** 4.3.3 and Higher	**IBM** FC 6204 HVD Ultra PCI; FC 6207 HVD Ultra PCI; FC 6205 LVD Ultra2 PCI; FC 6203 LVD/SE Ultra3 (PCI); Integrated Ultra2 SCSI LVD with VHDCI[1]; Integrated Ultra3 SCSI LVD with VHDCI[2]
Notes		

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1439
Doc. 3698

10408 A

Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information

1. Integrated LVD adapter with AIX 4.3.3 or higher on 7044 models 170 & 270, pSeries 620 (7025-6F1) & (7025-6F0), 7025 model F80, pSeries 640 (7026-B80), pSeries 660 (7026-6H1) & (7026-6H0) & (7026-6M1), 7026 models H80 & M80. For **6203 & 6204**, pSeries 670 (7040-671) through I/O drawer (7040-61D), pSeries 690 (7040-681) through I/O drawer (7040-61D), 9112-265.
2. Integrated Ultra 3 SCSI LVD adapter with AIX 4.3.3 or higher on pSeries 610 (7028-6C1) & (7028-6E1), 9112-265.
3. AIX 5.1 requires Atape driver level 6.1.4.0 or above; Level 7.0.6.0 or above recommended for the latest Ultrium timeout values.

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters/SAN**
Servers that support the listed host adapters.	**AIX** 4.3.3 and Higher	Click here for details.

Notes

Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.
2. AIX 5.1 requires Atape driver level 6.1.4.0 or above; Level 7.0.6.0 or above recommended for the latest Ultrium timeout values

Microsoft Windows NT, 2000, and 2003 Support

SCSI Ultrium LVD Ultrium 1 & Ultrium 2 and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
Servers that support the listed host adapters.	NT Server V4 with SP 6 (Ultrium 1 Only today) or Windows 2000 Build 2195	Adaptec AHA 2944 UW HVD Ult (PCI), or Netfinity Adapter #59H3900 HVD Ultra; Adaptec 29160 LVD Ultra160 PCI [1]; Adaptec 39160 LVD Ultra160 PCI [1];
	Or Windows 2003 Build 3790	Adaptec 2940 U2B LVD Ultra2 PCI or Netfinity Adapter #33L5000 Ultra2 SCSI PCI; Netfinity Adapter #19K4646 or Adaptec 29160LP [1&2]; Adaptec 39320 LVD Ultra320 PCI ——— LSI Logic Sym 22910 LVD Ultra2 PCI
Notes		

10407
A

1. **Supported with Restrictions.** See ftp://ftp.software.ibm.com/storage/devdrvr/Windows/Win2000/IBMUltrium.Win2K.Readme.txt or ftp://ftp.software.ibm.com/storage/devdrvr/Windows/Win2003/IBMUltrium.W2K3.Readme.tx or ftp://ftp.software.ibm.com/storage/devdrvr/Windows/WinNT/IBMUltrium.Win2K.Readme.txt for instructions.
2. Netfinity Adapter #19K4646 SCSI PCI Adapter made by Adaptec for IBM Netfinity.
3. See the Host Bus Adapter Supported Fibre Versions Matrix for the latest HBA support information, and the LTO Device Drivers for the latest device driver downloads.

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters/SAN**
Servers that support the listed host adapters.	NT Server V4 with SP6A or later (SDG 8005 with Ultrium 1 Only at this time) or Windows 2000 Build 2195 Or Windows 2003 Build 3790	Click here for details.

Notes

Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.

SUN Systems

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
SUN SPARC, UltraSPARC, and **Ultra/Enterprise Servers** that support the listed host adapters.	**Solaris** 7, 8, and 9	**SUN** X1065A HVD Ultra Sbus; X6541A [1] HVD Ultra PCI;
		X2222A LVD Ultra PCI

Notes

1. SUN Adapter X 6541 requires a VHDC1 interposer/cable; feature code 5099 on the 3583.

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters**

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1440
Doc 3698

SUN SPARC, UltraSPARC, and **Ultra/Enterprise Servers** that support the listed host adapters.	**Solaris** 7, 8, and 9	Click here for details.

Notes
Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information 1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.

Linux Support

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
32-bit Intel based	RedHat 7.2 with kernel 2.4.9-31 (Ultrium1 Only) RedHat 7.3 (Ultrium 1 Only) Advanced Server 2,1; SuSE Linux Enterprise Server 7 Update	LVD: Adaptec AHA 2944 UW; HVD: Adaptec 29160[3]; HVD Adaptec 39160[3]; HVD Adaptec 2940 U2W
Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models[1]		
Servers	**Operating Systems**	**Host Adapters/SAN**
	RedHat 7.2 with kernel 2.4.9-31 (SDG & Ultrium 1 Only);	
32-bit Intel based	RedHart 7.3 (Ultrium 1 Only); RedHat Advanced Server 2.1; SuSE Linus Enterprise Server 7 Update	Click here for details
64-bit Intel based	RedHat Advanced Server 2,1 (SDG & Ultrium1 Only);	Click here for details
Notes		

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.
2. For more details on IBM tape device drivers and drive microcode levels click here.
3. **Supported with Restrictions.** See ftp://ftp.software.ibm.com/storage/devdrvr/Linux/RHLAS2.1/IBMtape_Ultrium.Readme.txt for instructions.

10405
A

Additional Product Information is available:
IBM TotalStorage Ultrium Scalable Tape Library 3583 Setup, Operator Guide (GA32-0411).

The 3583 Ultrium Scalable Tape Library is supported by a variety of applications from Independent Software Vendors.

General Notes:

Attachment of LTO Ultrium 2 Tape Drives with the Adaptec SCSI Card 29160 or Adaptec 39160, installed in 32 bit PCI slots, is not supported.

All information on this page is provided by IBM on an "AS IS" basis only. IBM provides no warranty of compatibility. Individual results may vary based on environment.

Use of information that is provided by IBM is at the recipient's own risk. IBM provides no assurances that any reported problems may be resolved with the use of any information that IBM provides. By furnishing information, IBM does not grant any licenses to any copyrights, patents or any other intellectual property rights.

(c) International Business Machines Corporation 2003.

Any trademarks and product or brand names referenced in this document are the property of their respective owners. Please consult your IBM product manuals for complete trademark information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1441
3698
Doc.

10404
A.

Manual 09

IBM Tivoli
Storage Area Network Manager
Guia do Usuário Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
1442
Fls Nº
3698
Doc.

IBM Tivoli Storage Area Network Manager

Guia do Usuário

Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1443
3698
Doc
SC17-2576-01

IBM Tivoli Storage Area Network Manager

10403
A-

IBM

Guia do Usuário

Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
1444
Fls. Nº
S517-7576-01
3698
Doc

104.20
A.

Nota!
Antes de utilizar estas informações e o produto a que se referem, assegure-se de ler as informações gerais no Apêndice D, "Avisos", na página 83.

Segunda Edição (Abril de 2003)

Esta edição aplica-se à versão 1, release 2, modificação 0 do IBM Tivoli Storage Area Network Manager (números do programa 5698-SRE e 5698-SRS) e a quaisquer releases subseqüentes até que seja indicado o contrário em novas edições.

As alterações desde a edição anterior são marcadas com uma barra vertical (|) na margem esquerda. Assegure-se de que está utilizando a edição correta para o nível do produto.

Solicite publicações por meio de seu representante de vendas ou pela filial que atende a sua localidade.

O seu feedback é importante para ajudar a fornecer informações mais precisas e de melhor qualidade. Se você tiver comentários sobre esse manual ou qualquer outra documentação do IBM Tivoli Storage Area Network Manager, consulte "Entrando em Contato com o Suporte ao Cliente" na página vii.

© Copyright International Business Machines Corporation 2002, 2003. Todos os direitos reservados.

10399
A.

Índice

Prefácio v
Quem Deve Ler Este Guia v
Publicações v
Publicações do IBM Tivoli Storage Area Network Manager v
Publicações Relacionadas vi
Acessando Publicações On-line vi
Solicitando Publicações vi
Fornecendo Feedback sobre Publicações vi
Acessibilidade vii
Entrando em Contato com o Suporte ao Cliente . . vii
Relatando um Problema viii
Convenções Utilizadas Neste Guia viii
Convenções de Tipos viii

Resumo das Alterações para o IBM Tivoli Storage Area Network Manager Versão 1 ix
Alterações Técnicas para a Versão 1 Release 2 – Abril de 2003 ix

Parte 1. Fundamentos Básicos . . . 1

Capítulo 1. Introduzindo o IBM Tivoli Storage Area Network Manager. 3
Gerenciamento da Rede da Área de Armazenamento 4
Discovery 4
Exibições da Topologia 5
Eventos do SNMP 6
Detecção de Erros e Isolamento de Falhas . . . 6
Suporte a Internet SCSI 6
Interfaces para o Tivoli Storage Area Network Manager 8
Visão Geral das Tarefas do Administrador 8
Gerenciamento da SAN 8
Detecção de Problemas 10

Capítulo 2. Administrando o Tivoli Storage Area Network Manager 11
Gerenciando a Segurança do Sistema de Arquivos 11
Configurando e Exibindo Logs de Mensagens . . . 11
Configurando e Exibindo o Arquivo de Propriedades do Usuário 12
Iniciando a Interface com o Usuário do IBM Tivoli Storage Resource Manager 12

Capítulo 3. Exibindo a Rede 15
Iniciando a Interface Gráfica com o Usuário do Tivoli Storage Area Network Manager 15
Configurando os Agentes 16
Configurando o Destino de Eventos 19
Planejando Polling 21
Exibindo a Ajuda On-line 22
Selecionando e Interpretando Exibições da Rede . . 22
Exibição da SAN 23
Exibição Central do Host 26
Exibição Central do Dispositivo 27
Exibindo as Propriedades do Dispositivo da SAN 29
Alterando a Propriedade do Rótulo para um Símbolo 32
Compreendendo o Status 33
Como o Status se Propaga 34
Status na Exibição Gráfica do Submapa 35
Status na Exibição de Exploração do Submapa . . 35
Limpando o Histórico de Status 36
Filtragem do Status 37
Descobrindo Dispositivos iSCSI 37
Iniciando a Descoberta iSCSI 38
Replanejando o Polling iSCSI 40
Parar o Polling iSCSI 40

Capítulo 4. Trabalhando com Recursos 41
Iniciando Aplicativos de Dispositivos de Rede . . . 41
Uma Técnica Alternativa de Início 41
Utilizando SNMP para Gerenciar Eventos 43
Utilizando Detecção de Erros e Isolamento de Falhas 44
Iniciando e Parando o EDFI 45
Relatório de Eventos EDFI 46
Trabalhando com Conjuntos de Regras 47
Gerenciando um Evento EDFI 48

Parte 2. Apêndices 55

Apêndice A. Referência de Comandos 57
Lendo Diagramas de Sintaxe 57
Inserindo Comandos 60
Comandos de Serviço de Registro 61
srmcp log get 62
srmcp log help 63
srmcp log set 64
Comandos de Service Manager 66
srmcp ConfigService display 67
srmcp ConfigService get 68
srmcp ConfigService help 69
srmcp ConfigService set 70
srmcp ConfigService setAuthenticationPw . . . 72
srmcp ConfigService setPw 73

Apêndice B. Comando do Tivoli NetView 75
nvsniffer 76

Apêndice C. Detecção de Problemas 77
Verificando Arquivos de Log 77
Detecção de Problemas de Gerenciamento da SAN 78

Apêndice D. Avisos 83

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls - Nº 1445
Doc. 3698

1039
A

Prefácio

O IBM Tivoli Storage Area Network Manager gerencia todos os seus dispositivos em uma SAN (Rede da Área de Armazenamento). As capacidades incluem discovery, monitoração, disponibilidade e gerenciamento de eventos. Este guia descreve como gerenciar os recursos em sua Rede da Área de Armazenamento.

Quem Deve Ler Este Guia

Esta publicação destina-se a administradores da SAN e a operadores da rede que precisam gerenciar o IBM Tivoli Storage Area Network Manager. Os leitores devem estar familiarizados com os seguintes tópicos:

- DB2 (Database 2)
- Conceitos da SAN
- Conceitos do SNMP (Simple Network Management Protocol)
- Tivoli Enterprise Console
- Tivoli NetView

Publicações

Esta seção lista as publicações na biblioteca do IBM Tivoli Storage Area Network Manager e quaisquer outros documentos relacionados. Descreve também como acessar as publicações on-line do Tivoli, como solicitar publicações do Tivoli e como submeter comentários sobre publicações do Tivoli.

Publicações do IBM Tivoli Storage Area Network Manager

A tabela a seguir lista as publicações do IBM Tivoli Storage Area Network Manager.

Título da Publicação	Número de Ordem
IBM Tivoli Storage Area Network Manager: Guia do Usuário	S517-7576
IBM Tivoli Storage Area Network Manager Planning and Installation Guide	SC23-4697
IBM Tivoli Storage Area Network Manager Messages	SC32-0953

A biblioteca do Tivoli Storage Area Network Manager em todos os idiomas traduzidos está disponível no seguinte CD-ROM:

Título	Número de Ordem
IBM Tivoli Storage Area Network Manager Publications CD-ROM	SCD7-0463

As publicações também estão disponíveis no site de publicações Tivoli, na Web: http://www-3.ibm.com/software/tivoli/library/

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1446
3698
Doc.

Publicações Relacionadas

A tabela a seguir lista as publicações relacionadas de produtos IBM.

Título	Número de Ordem
Introduction to Rede da Área de Armazenamento, SAN	SG24-5470
Designing an IBM Storage Area Network	SG24-5758
NetView for Windows NT Programmer's Reference	SC31-8890
NetView for Windows User's Guide	SC31-8888

O *Tivoli Software Glossary* inclui definições para muitos dos termos técnicos relacionados a software Tivoli. O *Tivoli Software Glossary* está disponível, somente em inglês, no seguinte Web site:

http://publib.boulder.ibm.com/tividd/glossary/termsmst04.htm

Acessando Publicações On-line

Você pode acessar as publicações no Tivoli Information Center a partir do seguinte Web site de Suporte ao Cliente:

http://www-3.ibm.com/software/tivoli/library/

O Tivoli Information Center contém a versão mais recente dos manuais da biblioteca de produtos nos formatos PDF ou HTML, ou em ambos. Os documentos traduzidos também estão disponíveis para alguns produtos.

Nota: Se você imprimir documentos em PDF em papel que não seja do tamanho carta, selecione a caixa de opções **Ajustar à página**, no diálogo **Impressão no Adobe Acrobat**. Essa opção estará disponível quando você clicar em **Arquivo → Imprimir**. A opção **Ajustar á página** assegura que as dimensões totais de uma página do tamanho carta sejam impressas no papel que você está utilizando.

Solicitando Publicações

Você pode solicitar várias publicações on-line do Tivoli no seguinte Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

Também pode solicitar por telefone, ligando para um destes números:

- Nos Estados Unidos: 800-879-2755
- No Canadá: 800-426-4968

Em outros países, consulte o seguinte Web site para obter uma lista de números de telefone:

http://www.ibm.com/software/tivoli/order-lit/

Fornecendo Feedback sobre Publicações

Se você tiver comentários ou sugestões sobre os produtos e a documentação do Tivoli, envie um e-mail para pubs@tivoli.com ou preencha a pesquisa de feedback do cliente no seguinte Web site:

http://www.ibm.com/software/tivoli/contact.html/

Acessibilidade

Os recursos de acessibilidade ajudam um usuário que tem uma deficiência física, como por exemplo mobilidade restrita ou visão limitada, a utilizar produtos de software com êxito. Com este produto, você pode utilizar tecnologias de apoio para ouvir e navegar na interface. Também é possível utilizar o teclado em vez do mouse para operar todos os recursos da interface gráfica com o usuário.

Para obter informações adicionais, consulte o Apêndice Acessibilidade no *IBM Tivoli Storage Area Network Manager Planning and Installation Guide.*

Entrando em Contato com o Suporte ao Cliente

Para obter suporte referente a esse ou qualquer outro produto Tivoli, você pode entrar em contato com o suporte ao cliente IBM de uma das seguintes maneiras:

- Visite o site de suporte técnico do IBM Tivoli Storage Area Network Manager na Web em http://www.ibm.com/software/support/.
- Submeta eletronicamente um PMR (registro de gerenciamento de problemas) em **IBMSERV/IBMLINK**. É possível acessar o IBMLINK no endereço http://www2.ibmlink.ibm.com.
- Envie um PMR eletronicamente no endereço http://www.ibm.com/software/sysmgmt/products/support/. Consulte "Relatando um Problema" na página viii para obter detalhes.

Clientes nos Estados Unidos também podem telefonar para 1-800-IBM-SERV (1-800-426-7378).

Os clientes internacionais devem consultar o Web site para obter os números de telefone de suporte ao cliente.

Clientes com deficiência auditiva devem visitar o Web site do TDD/TTY Voice Relay Services and Accessiblity Center no endereço http://www.ibm.com/able/voicerelay.html.

Você também pode consultar o *IBM Software Support Handbook,* que está disponível em nosso Web site no endereço http://techsupport.services.ibm.com/guides/handbook.html.

Ao entrar em contato com o suporte ao cliente, esteja preparado para fornecer informações de identificação de sua empresa, para que a equipe de suporte possa ajudá-lo prontamente. As informações de identificação da empresa também podem ser necessárias para acessar diversos serviços on-line disponíveis no Web site.

O Web site de suporte oferece informações completas, incluindo um guia para serviços de suporte (o IBM Software Support Handbook), as FAQs (perguntas mais freqüentes) e a documentação de todos os produtos de Software IBM, como Release Notes, Redbooks e Documentos Técnicos. A documentação para alguns releases do produto está disponível nos formatos PDF e HTML. Documentos traduzidos também estão disponíveis para alguns releases do produto.

Todas as publicações do Tivoli estão disponíveis para download eletrônico ou podem ser solicitadas no IBM Publications Center:http://www-3.ibm.com/software/tivoli/library/

1039
A
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1447
Doc 3698

Estamos muito interessados em saber sobre sua experiência com os produtos e a documentação do Tivoli. Suas sugestões de melhorias também são bem-vindas. Se você tiver comentários ou sugestões sobre nossa documentação, preencha nosso questionário de feedback do cliente no endereço:

`http://www-3.ibm.com/software/sysmgmt/products/support/Tivoli_Escalation_Process.html`

Relatando um Problema

Tenha as seguintes informações prontas ao comunicar um problema:

- O número da versão, do release, da modificação e do nível de serviço do IBM Tivoli Storage Area Network Manager.
- O número do protocolo de comunicação (por exemplo, TCP/IP), da versão e do release que você está utilizando.
- A atividade que você estava executando quando o problema ocorreu, listando as etapas seguidas antes de o problema ocorrer.
- O texto exato de quaisquer mensagens de erro.

Convenções Utilizadas Neste Guia

Este manual utiliza várias convenções para determinados termos e ações, comandos e caminhos que dependem do sistema operacional e gráficos de margem.

Convenções de Tipos

As seguintes convenções de tipos são utilizadas neste manual:

Negrito Comandos em letras minúsculas e com letras maiúsculas e minúsculas misturadas, opções de comandos e sinalizadores que aparecem no texto são exibidos **assim, em negrito**.

Elementos da interface gráfica com o usuário (exceto para títulos de janelas e diálogos) e nomes de teclas também são exibidos **assim, em negrito**.

Itálico As variáveis, valores que você deve fornecer, novos termos e palavras e frases que são enfatizados são exibidos *assim, em itálico*.

`Espaçamento fixo`

Os comandos, as opções de comandos e os flags que aparecem em uma linha separada, os exemplos de códigos, as saídas e o texto da mensagem são exibidos `assim, em espaçamento fixo`.

Os nomes de arquivos e diretórios, as cadeias de texto que você deve digitar, quando aparecerem dentro do texto, os nomes de métodos e classes Java e as marcações em HTML e XML também são exibidos `assim, em espaçamento fixo`.

Resumo das Alterações para o IBM Tivoli Storage Area Network Manager Versão 1

Esta seção resume as alterações que foram feitas no produto e nesta publicação.

Alterações Técnicas para a Versão 1 Release 2 – Abril de 2003

As seguintes alterações foram feitas no produto para esta edição:

EDFI (Detecção de Erro e Isolamento de Falha)

A função EDFI fornece ajuda com determinação de problemas em links de interconexão SAN Fibre Channel. O EDFI utiliza análise de falhas previstas e fornece capacidades de isolamento de falhas que permitem identificar e tomar a ação apropriada para componentes que possam estar falhando.

Para obter informações adicionais, consulte "Utilizando Detecção de Erros e Isolamento de Falhas" na página 44 e também o *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

WebSphere Application Server - Express, Versão 5.0 incorporado

A instalação do IBM Tivoli Storage Area Network Manager inclui a versão incorporada do WebSphere Application Server - Express. Uma instalação separada do WebSphere não é mais necessária.

Suporte a Internet SCSI (iSCSI)

O Tivoli Storage Area Network Manager fornece suporte básico para descoberta e monitoração de dispositivos iSCSI através do Tivoli NetView. iSCSI permite que protocolos de E/S em bloco (comandos, seqüências e atributos) sejam enviados por uma rede usando o protocolo TCP/IP.

Para obter informações adicionais, consulte "Descobrindo Dispositivos iSCSI" na página 37 e também o *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

Suporte de sistema operacional foi adicionado para os seguintes componentes:

- Host gerenciado no AIX 5.2
- Host gerenciado no Linux Redhat Advanced Server v2.1
- Host gerenciado no Suse Linux Enterprise Server 7.0
- Console remoto NetView no Windows XP
- Tivoli Storage Area Network Manager no AIX 5.1. Este suporte não inclui o Tivoli NetView. É preciso utilizar um console remoto do Windows 2000 ou Windows XP para o Tivoli Storage Area Network Manager no AIX.

Consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* para obter mais informações.

Endereços IP dinâmicos para hosts gerenciados e consoles remotos

É possível especificar endereços IP dinâmicos em vez de endereços IP estáticos para hosts gerenciados e consoles remotos.

Nota: O gerenciador ainda exige um endereço IP estático.

© Copyright IBM Corp 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1448
3698
Doc.

Identificação da SAN

O Tivoli Storage Area Network Manager agora exibe o nome da SAN ao qual um objeto está conectado.

Classes de eventos adicionais do Tivoli Enterprise Console

O Tivoli Storage Area Network Manager fornece classes de eventos TEC adicionais que permitem filtrar facilmente eventos com base no tipo de evento TEC. Consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* para obter mais informações.

Suporte à chave Cisco Série MDS 9000

O IBM Tivoli Storage Area Network Manager aprimorou a compatibilidade para a chave Cisco Série MDS 9000. O NetView exibe os números das portas em um formato de SSPP, em que *SS* é o número do slot e *PP* é o número da porta. O item do menu Ativar Aplicativo está disponível para a chave Cisco. Quando Ativar Aplicativo é selecionado o aplicativo Cisco Fabric Manager é iniciado.

Versões de Agente

Um agente do IBM Tivoli Storage Area Network Manager Release 1 em um host gerenciado pode coexistir com um gerenciador do Release 2. O Tivoli Storage Area Network Manager acompanha as diferenças de funcionalidade entre um agente do Release 1 e um agente do Release 2 e toma a ação apropriada com base nessas informações. Por exemplo, um agente do Release 1 não suporta a nova função, como EDFI. Você não pode instalar um agente do Release 1 e um do Release 2 no mesmo host gerenciado.

Suporte a Console Remoto no Windows XP

O console remoto do IBM Tivoli Storage Area Network Manager agora é suportado no Windows XP. O Tivoli NetView 7.1.3 é exigido para suportar o Windows XP.

Novos Ícones para Entrada Manual

Quando for executada a entrada manual em dispositivos desconhecidos, os seguintes ícones estarão disponíveis:

- ESS
- Controlador de Volume SAN

1039

Parte 1. Fundamentos Básicos

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
FTs Nº 1449
Doc. 3698

10390
A.

Capítulo 1. Introduzindo o IBM Tivoli Storage Area Network Manager

O Tivoli Storage Area Network Manager o ajuda a gerenciar os seus recursos, fornecendo capacidades de discovery e gerenciamento de recursos da rede.

A Figura 1 mostra como o Tivoli Storage Area Network Manager pode gerenciar todos os seus recursos de armazenamento. Isso inclui os dispositivos conectados aos sistemas host por meio de hubs com base em fibras, pontes, comutadores, roteadores, gateways e diretores. O Tivoli Storage Area Network Manager também gerencia quaisquer hosts com agentes.

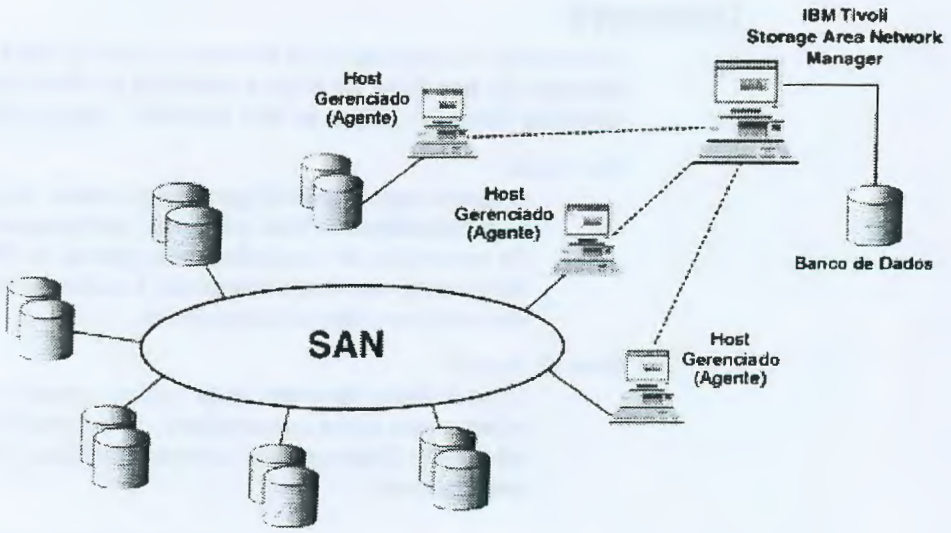


Figura 1. O IBM Tivoli Storage Area Network Manager em um ambiente de rede da área de armazenamento

Com o Tivoli Storage Area Network Manager, um sistema age como o gerenciador e um ou mais outros sistemas são os hosts gerenciados:

Gerenciador

O gerenciador faz o seguinte:

- Reúne dados dos agentes em hosts gerenciados, como descrições de SANs (Redes da Área de Armazenamento), LUNs (Números de Unidade Lógica) e informações sobre o sistema de arquivos e o host.
- Fornece exibições gráficas da topologia da SAN.
- Gera eventos SNMP (Simple Network Management Protocol) quando uma alteração for detectada na estrutura da SAN.
- Transfere eventos para o Tivoli Enterprise Console ou um console do SNMP.

Hosts gerenciados

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1450
3698
Doc.

Um agente reside em cada host gerenciado. Os agentes dos hosts gerenciados fazem o seguinte:

- Reunem informações sobre a SAN, consultando comutadores e dispositivos para obtenção de informações sobre o atributo e a topologia.
- Reúnem informações no nível do host, como sistemas de arquivos e mapeamento para LUNs.
- Reunem informações sobre o evento e outras informações detectadas pelos HBAs (Adaptadores de Barramento do Host).

Gerenciamento da Rede da Área de Armazenamento

O gerenciamento da SAN descobre automaticamente os componentes e dispositivos da SAN, e exibe a topologia de seu ambiente de SAN. Você pode monitorar a utilização do armazenamento na SAN e determinar a disponibilidade dos componentes da SAN.

Discovery

O processo de localização de recursos dentro de uma empresa, incluindo a detecção da topologia da rede, é chamada de *discovery*. O Tivoli Storage Area Network Manager utiliza os dois métodos a seguir para descobrir sua rede:

Na banda
O agente em cada host gerenciado coleta informações sobre a máquina host propriamente dita, incluindo informações sobre o sistema de arquivos. Os comandos são enviados pelas placas do HBA (Adaptador de Barramento do Host), anexando a máquina host à SAN para reunir informações sobre os dispositivos.

Fora da banda
O gerenciador também pode utilizar consultas do SNMP para descobrir informações sobre comutadores da estrutura selecionados. As informações sobre MIB (Management Information Base) são coletadas a partir desses comutadores.

Um discovery pode ser acionado por qualquer uma das seguintes ações:

- Um usuário solicita um discovery (executar poll agora).
- Ocorre um evento que faz com que o IBM Tivoli Storage Area Network Manager execute um discovery.
- Um discovery planejado ou periódico é iniciado. Um discovery planejado se torna padrão a cada 24 horas.
- Um host gerenciado ou um agente SNMP foi incluído.

A Tabela 1 na página 5 explica quando é executada uma descoberta completa e uma descoberta de topologia.

10388
A.

Tabela 1.

Tipos de Descoberta	Uma Descoberta É Executada Quando:
Completa Dependendo do número de objetos a descobrir, uma descoberta completa pode levar muito tempo para concluir. É possível especificar quando executar uma descoberta completa. Consulte "srmcp ConfigService set" na página 70.	• Um usuário pede uma descoberta (poll agora) • Uma descoberta planejada ou periódica é iniciada • Um host gerenciado é adicionado
Topologia Este tipo de descoberta leva menos tempo para executar do que uma descoberta completa. Entretanto, uma descoberta de topologia não atualiza as exibições centrais no host ou no dispositivo. Essas exibições são atualizadas quando um discovery completo for executado.	• Quando o IBM Tivoli Storage Area Network Manager é iniciado • Quando o IBM Tivoli Storage Area Network Manager detecta alterações na SAN • Quando um agente SNMP (chave) é adicionado

Os dados coletados de hosts gerenciados são armazenados no banco de dados DB2.

A coleta de dados é executada por planejamento e por eventos. Um planejamento aciona o discovery e o torna padrão a cada 24 horas. Quando o Tivoli Storage Area Network Manager detecta um evento em um comutador da estrutura, um novo discovery começa.

O Tivoli Storage Area Network Manager também suporta descoberta de iSCSI. A descoberta de iSCSI é executada independentemente da descoberta feita pelo Tivoli Storage Area Network Manager e exige que você ative a descoberta de IP do Tivoli NetView. Para obter informações adicionais consulte "Descobrindo Dispositivos iSCSI" na página 37 e *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

Exibições da Topologia

O Tivoli Storage Area Network Manager extrai informações sobre a estrutura a partir do banco de dados e utiliza o Tivoli NetView para exibir a topologia da estrutura. A Tabela 2 na página 6 descreve as exibições disponíveis para as SANs. Para cada dispositivo descoberto e exibido, você pode abrir um diálogo de propriedades que mostra os atributos e as conexões associadas a esse dispositivo.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1451
3698
Doc.

Tabela 2. Descrição de Exibições da SAN a partir do Tivoli NetView

Exibições da SAN	Descrição
Símbolos da SAN (do Submapa Raiz)	Exibe um símbolo para cada SAN. Dê um clique duplo em um símbolo da SAN para exibir o seu submapa. A partir de um submapa você pode optar por uma das seguintes exibições: • Exibição da Topologia: Exibe a SAN inteira com dois tipos de símbolos, um para os elementos da conexão da SAN e outro para cada segmento da estrutura. • Exibição das Zonas: Exibe a SAN como um agrupamento de zonas.
Central do Host	Exibe todos os sistemas host e suas relações lógicas com dispositivos locais e conectados à SAN. Não exibe os comutadores e outros dispositivos de conexão.
Central do Dispositivo	Exibe todos os dispositivos de armazenamento e suas relações lógicas com todos os hosts. Não exibe os comutadores e outros dispositivos de conexão.

Eventos do SNMP

O Tivoli Storage Area Network Manager pode enviar eventos, que representam uma alteração no estado da estrutura, para qualquer console do evento dentro da empresa do qual o Tivoli Storage Area Network Manager participa. Esses eventos são gerados nos formatos SNMP e Tivoli Enterprise Console.

Detecção de Erros e Isolamento de Falhas

O Tivoli Storage Area Network Manager fornece capacidades de EDFI (Detecção de Erros e Isolamento de Falhas) e pode relatar dispositivo de hardware com defeito em links de interconexão SAN Fibre Channel antes que se tornem falhas permanentes do dispositivo. EDFI pode executar análise de falhas previstas analisando contadores associados à transmissão de dados em links SAN.

O Tivoli Storage Area Network Manager fornece uma interface com o usuário EDFI a partir do console do Tivoli NetView que permite gerenciar notificações EDFI e conjuntos de regras. Os conjuntos de regras especificam limites e critérios usados pela análise de falhas previstas e funções associadas de isolamento de falhas do Tivoli Storage Area Network Manager.

O EDFI gera eventos padrões do Tivoli Enterprise Console que podem ser utilizados para fins de relatório. O EDFI relata componentes com falha no log de Propriedades de EDFI e como um símbolo EDFI no próprio dispositivo na interface de topologia do gerenciador de SAN. Observe que o EDFI isola as falhas no nível do link – qualquer lado do link ou o próprio cabo pode ser o componente com falha.

Para obter informações adicionais sobre EDFI, consulte "Utilizando Detecção de Erros e Isolamento de Falhas" na página 44 e *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

Suporte a Internet SCSI

O Tivoli Storage Area Network Manager fornece suporte básico para descoberta e monitoração de dispositivos iSCSI através do Tivoli NetView. iSCSI permite que protocolos de E/S em bloco (comandos, seqüências e atributos) sejam enviados por uma rede usando o protocolo TCP/IP.

A arquitetura SCSI é baseada em um modelo de cliente/servidor. A Internet SCSI leva esse modelo em conta ao fornecer pedidos de armazenamento por redes TCP/IP. O (*iniciador*) do cliente, em geral, é um sistema host tal como um servidor de arquivos que emite pedidos de leitura ou gravação. O (*destino*) do servidor é um recurso tal como uma matriz de discos que responde a pedidos do cliente.

O Tivoli Storage Area Network Manager fornece o seguinte suporte:

- Os dispositivos iSCSI que têm suporte a MIB iSCSI e a SNMP podem ser descobertos utilizando o console Tivoli NetView. O processo de descoberta cria automaticamente um SmartSet iSCSI que contém os dispositivos iSCSI como seus membros.
- O comando **nvsniffer** do Tivoli NetView pode ser emitido manualmente para descobrir dispositivos iSCSI. O comando especifica um arquivo de configuração que identifica quais dispositivos fornecem suporte iSCSI.
- Os arquivos de definição de traps MIB iSCSI são utilizados pelo processamento de eventos do Tivoli NetView tais como filtragem de eventos, encaminhamento, pager, e-mail e ações personalizadas.
- Os MIBs iSCSI e MIBs iSNS são instalados com o Tivoli Storage Area Network Manager e o administrador pode então carregar os MIBs utilizando o painel Carregador de MIB do Tivoli NetView.

  O suporte iSCSI do Tivoli Storage Area Network Manager pode ser utilizado independentemente ou em conjunto com a estrutura de gerenciamento iSNS (Internet Storage Naming Service). O protocolo iSNS é um protocolo para gerenciamento de dispositivos iSCSI. Se o iSNS for utilizado com o Tivoli Storage Area Network Manager, é possível carregar os arquivos de MIB iSNS e utilizar o navegador MIB do Tivoli NetView para consultar o servidor iSNS e exibir o status de dispositivos iSCSI. Para obter informações adicionais sobre iSCSI e iSNS, consulte o seguinte Web site:

  `http://www.ietf.org`

Descoberta iSCSI

É possível iniciar a descoberta iSCSI através do menu do Tivoli NetView. Somente dispositivos que suportam MIB SCSI MIB e SNMP podem ser descobertos e gerenciados. A descoberta iSCSI do Tivoli NetView ativa um comando **nvsniffer** que consulta se os dispositivos são dispositivos iSCSI. É possível utilizar o Tivoli NetView para descobrir: todos os dispositivos iSCSI, todos os iniciadores iSCSI ou todos os destinos iSCSI. Em seguida, o processo de descoberta cria um SmartSet que contém os dispositivos iSCSI descobertos. Para obter mais informações, consulte "Descobrindo Dispositivos iSCSI" na página 37.

A descoberta de dispositivo iSCSI exige que se ative a descoberta IP do Tivoli NetView, a definição padrão tem a descoberta IP desativada. Para obter informações sobre a ativação da descoberta IP consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

Também é possível iniciar ou parar a descoberta ISCSI a partir da interface da linha de comandos utilizando o comando **nvsniffer**. Para obter mais informações, consulte "nvsniffer" na página 76.

É possível controlar a descoberta da rede IP do Tivoli NetView criando um arquivo *inicial*. Um arquivo inicial contém uma lista de nomes de hosts ou endereços IP de nós SNMP em seu domínio administrativo. É possível utilizar um arquivo inicial para forçar o processo de descoberta a gerar o mapa da topologia começando de nós diferentes do sistema de gerenciamento. Para obter informações adicionais consulte o manual *NetView for Windows User's Guide*.

1038
A
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls - Nº 1452
Doc. 3698

Interfaces para o Tivoli Storage Area Network Manager

Esta seção descreve o tipo de interfaces disponíveis no Tivoli Storage Area Network Manager.

- Console do Tivoli NetView

  É possível utilizar o Tivoli NetView para exibir a topologia da malha, exibir os eventos no banco de dados de eventos e gerenciar notificações e conjuntos de regras de EDFI.

- Interface da linha de comando

  É possível utilizar a interface da linha de comandos para emitir comando de log, comandos de serviço do gerenciador ou quando se criam scripts que submetem comandos. Para obter mais informações, consulte o Apêndice A, "Referência de Comandos", na página 57.

Visão Geral das Tarefas do Administrador

As seções a seguir apresentam as tarefas do administrador para gerenciamento da SAN e detecção de problemas.

Gerenciamento da SAN

Para gerenciar uma Rede da Área de Armazenamento, um administrador pode utilizar o Tivoli Storage Area Network Manager para executar as seguintes tarefas a partir do Console do Tivoli NetView. Para obter mais informações, consulte o Capítulo 3, "Exibindo a Rede", na página 15.

- Configurar agentes

  Os agentes são utilizados para descobrir sua SAN e monitorar o seu status. Utilize o painel **Configuração do Agente** para fazer o seguinte:

  - Exibir e remover agentes inativos na banda
  - Exibir, incluir, remover e configurar agentes fora da banda

  Consulte o Capítulo 3, "Exibindo a Rede", na página 15 para obter mais informações.

- Configurar destino do evento

  Você pode utilizar o Tivoli NetView Event Browser para exibir eventos no banco de dados de eventos do Tivoli NetView. Você pode configurar o destino de traps do SNMP e eventos TEC. Os seguintes tipos de informações podem ser encontrados no banco de dados de eventos:

  - Condições que o NetView detecta, como um dispositivo em status crítico
  - Traps do SNMP enviados de dispositivos na rede IP
  - Traps do SNMP enviados de dispositivos da SAN, como um Comutador Fibre Channel
  - Traps do SNMP enviados do Tivoli Storage Area Network Manager

  Para obter informações sobre como configurar destinos de eventos, consulte "Configurando o Destino de Eventos" na página 19 e "Utilizando SNMP para Gerenciar Eventos" na página 43.

- Iniciar o discovery de sua SAN

  O Tivoli Storage Area Network Manager descobre a topologia da estrutura de sua SAN, efetuando o polling dos agentes. Você pode efetuar o poll de informações da SAN imediatamente ou o polling do planejamento. O tempo necessário para concluir o polling depende do tamanho de sua rede da área de

10384
A.

armazenamento. As informações sobre topologia são armazenadas em um banco de dados DB2. Para obter mais informações, consulte "Planejando Polling" na página 21.

O Tivoli Storage Area Network Manager pode descobrir seus dispositivos iSCSI e criar e manter SmartSets em uma base planejada regularmente. Opcionalmente, é possível descobrir os dispositivos iSCSI e planejar o polling a partir da interface da linha de comandos. Para obter mais informações, consulte "Descobrindo Dispositivos iSCSI" na página 37.

- Selecionar e interpretar exibições das SANs

  Utilizando o Console do Tivoli NetView, você pode optar por exibir a SAN em uma exibição em modo gráfico ou de exploração do submapa. Se preferir, poderá optar por mostrar as duas exibições.

  Dentro da exibição da SAN, as seguintes exibições estão disponíveis: Topologia, Zona, Central do Host e Central do Dispositivo.

  É possível exibir informações sobre propriedade do dispositivo da SAN a partir da exibição central do dispositivo. Também é possível exibir informações sobre conexão dos comutadores Fibre Channel e informações sobre sensores de um dispositivo.

  O Tivoli Storage Area Network Manager permite alterar os rótulos e os ícones de determinados dispositivos na exibição da topologia. Isso lhe dá flexibilidade para tornar a exibição mais fácil de ler e entender.

  O status de um dispositivo é refletido na cor do símbolo. Um símbolo pode representar um dispositivo ou um submapa. Se o símbolo for um submapa, o status refletirá no primeiro submapa filho.

  Para obter mais informações, consulte o Capítulo 3, "Exibindo a Rede", na página 15.

- Iniciar aplicativos do dispositivo de rede

  Alguns dispositivo de rede, como os comutadores Fibre Channel e os dispositivos de armazenamento, contêm aplicativos com base no navegador para ajudá-lo a configurar e gerenciar esses dispositivos. Se um dispositivo tiver um aplicativo de gerenciamento identificado para o Tivoli Storage Area Network Manager, você será capaz de iniciar o aplicativo a partir do menu do console. Alguns dispositivos SAN têm aplicativos de gerenciamento, mas não suportam a arquitetura para identificar o nome do aplicativo. O Tivoli Storage Area Network Manager fornece um método alternativo para exibir esses dispositivos. Para obter mais informações, consulte o Capítulo 4, "Trabalhando com Recursos", na página 41.

- Utilizar o SNMP para gerenciar eventos

  Você pode utilizar o Tivoli NetView Event Browser para exibir eventos no banco de dados de eventos do Tivoli NetView. O banco de dados de eventos pode conter eventos para as redes com base em IP e para as SANs. Para obter mais informações, consulte "Utilizando SNMP para Gerenciar Eventos" na página 43.

- Utilize EDFI para gerenciar problemas de hardware em links de interconexão SAN Fibre Channel

  EDFI fornece análise de falhas previstas e isolamento de falhas para identificar um componente com falha. Utilize o painel **Configuração ED/FI** para fazer o seguinte:

  - Ativar ou desativar EDFI
  - Especificar um conjunto de regras que contenha limites e critérios específicos a serem utilizados pelo Tivoli Storage Area Network Manager

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1453
Doc. 3698

Quando um evento EDFI for reportado, você pode gerenciar o evento fazendo o seguinte:

- Localize a Notificação de Erro EDFI no console do gerenciador SAN
- Utilize a Notificação de Erro EDFI para localizar o link que falhou
- Utilize diagnósticos específicos do dispositivo e guias de determinação de problemas para isolar o componente com falha no link
- Planeje um horário para substituir o componente apropriado
- Limpe a notificação de erro depois que o componente for substituído ou reparado.

O DB2 (Database 2) UDB (Universal Database) é fornecido com o Tivoli Storage Area Network Manager. As informações sobre topologia são armazenadas em um banco de dados DB2. Para assegurar a recuperação de dados da topologia da SAN, no caso de perda do banco de dados, recomenda-se fazer backup regularmente do banco de dados DB2. Você pode utilizar qualquer um dos recursos de backup do DB2 disponíveis para fazer o backup do banco de dados.

Detecção de Problemas

Há ajuda disponível para possíveis problemas que você poderá encontrar no gerenciamento da SAN. Para obter mais informações, consulte o Apêndice C, "Detecção de Problemas", na página 77.

10382
A

Capítulo 2. Administrando o Tivoli Storage Area Network Manager

Depois que o Tivoli Storage Area Network Manager estiver instalado, um administrador pode querer executar as seguintes tarefas:

- Gerenciar a segurança do sistema de arquivos.
- Configurar o log de mensagens para exibição.
- Configurar e exibir o arquivo de propriedades do usuário.
- Iniciar a interface com o usuário do Tivoli Storage Resource Manager.

Gerenciando a Segurança do Sistema de Arquivos

A segurança do Tivoli Storage Area Network Manager depende de um sistema de arquivos seguro, pois as informações sensitivas, como senhas de keystore de certificado e propriedades de configuração permanecem no gerenciador e nos hosts gerenciados. Você deve utilizar a segurança do sistema de arquivos para controlar o acesso a essas informações.

- Uma instalação do gerenciador e do agente em Windows devem existir em um sistema de arquivos NTFS.
- O administrador do sistema (usuário raiz) de uma máquina sempre deverá ter acesso ao sistema de arquivos local. Portanto, você deve controlar o acesso raiz em máquinas que estejam executando o software Tivoli Storage Area Network Manager.
- Muitos arquivos devem ter acesso restrito por razões de segurança. Por exemplo:
  - Arquivo services.properties
  - Diretório <install_dir>/lib
  - Arquivo setenv.bat
  - setenv.sh para o ambiente do gerenciador AIX
  - Arquivo server.xml
  - Arquivo tsnmdbparms.properties

Configurando e Exibindo Logs de Mensagens

O Tivoli Storage Area Network Manager emite quatro tipos de mensagens: Informativas, Aviso, Erro e Decisão. Essas mensagens são registradas em arquivos de texto que você pode exibir com um programa de edição padrão, como o Windows Notepad. Por padrão, os arquivos de log estão localizados no diretório <dir_instalação>/log nas máquinas do gerenciador, agente, e console remoto, consulte "Verificando Arquivos de Log" na página 77.

Antes de utilizar o Tivoli Storage Area Network Manager, você deve configurar os logs de mensagens. A partir de qualquer gerenciador, host gerenciado ou máquina de console remoto, você pode emitir comandos para fazer o seguinte:

- Efetuar logon ou logoff a qualquer momento. Por padrão, o registro de mensagens está ativado.
- Alterar a localização dos arquivos de log.

© Copyright IBM Corp 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1454
3698
Doc.

- Configurar filtros, de modo que apenas determinados tipos de mensagens sejam registradas. Por exemplo, você pode querer que apenas mensagens de erro e de aviso sejam registradas, mas não mensagens informativas.
- Especificar o número de arquivos de log files desejado. Isso é útil para assegurar que você possa reter os históricos dos logs. Por exemplo, se você tiver apenas um arquivo de log e ele ficar cheio, as entradas de log serão excluídas, à medida que novas entradas forem inseridas no arquivo. Se você tiver dois ou mais arquivos de log, poderá reter mais registros de log antigos. Você também pode definir o tamanho máximo de um arquivo de log.

Para obter detalhes sobre inserção de comandos, consulte "Inserindo Comandos" na página 60. Para obter detalhes sobre a sintaxe de comandos, consulte "Comandos de Serviço de Registro" na página 61.

Como os arquivos de log ficam cada vez maiores, faça backups ocasionais em outra máquina ou em uma mídia, ou exclua esses arquivos.

Configurando e Exibindo o Arquivo de Propriedades do Usuário

O arquivo de propriedades do usuário na máquina do gerenciador (`tivoli/itsanm/manager/conf/user.properties`) contém definições que controlam polling, destino de traps SNMP e o nome de host completo do IBM Tivoli Storage Area Network Manager. Como um administrador, você pode utilizar um conjunto de comandos para exibir e definir os valores no arquivo de propriedades do usuário. Você pode definir os seguintes valores:

- O dia da semana e a hora para polling.
- O intervalo no qual o polling do host ocorre.
- O intervalo de monitoração do agente fora da banda.
- O número da porta para traps do SNMP.
- O nome da comunidade do SNMP.
- O nome de host completo da máquina IBM Tivoli Storage Resource Manager.

Também há ajuda sobre como utilizar os comandos do Manager Service. Para obter detalhes sobre os comandos, consulte "Comandos de Service Manager" na página 66.

Iniciando a Interface com o Usuário do IBM Tivoli Storage Resource Manager

Se o IBM Tivoli Storage Resource Manager estiver instalado, poderá ser iniciado utilizando o console Tivoli NetView do Tivoli Storage Area Network Manager. O arquivo de propriedades do usuário contém uma definição SRMURL cujo padrão é o nome de host completo do Tivoli Storage Area Network Manager. Esse padrão supõe que o IBM Tivoli Storage Resource Manager e o Tivoli Storage Area Network Manager estão instalados na mesma máquina. Se o IBM Tivoli Storage Resource Manager estiver instalado em uma máquina separada, será possível modificar o valor de SRMURL para especificar o nome do host da máquina IBM Tivoli Storage Resource Manager. Para obter informações adicionais sobre a definição do valor de SRMURL, consulte "srmcp ConfigService set" na página 70.

Se as condições a seguir forem verdadeiras, você pode iniciar a interface gráfica do Tivoli Storage Resource Manager a partir do console do Tivoli NetView:

- O IBM Tivoli Storage Resource Manager ou a interface gráfica do Tivoli Storage Resource Manager está instalado na mesma máquina que o Tivoli Storage Area Network Manager ou o valor de SRMURL especifica o nome do host do IBM Tivoli Storage Resource Manager.
- O Tivoli Storage Area Network Manager está em execução no momento.

Este é o procedimento para iniciar a interface:

- Clique no ícone do Tivoli NetView, no desktop. O console do Tivoli NetView será exibido.
- Selecione **SAN → Storage Resource Manager**, no console do Tivoli NetView.

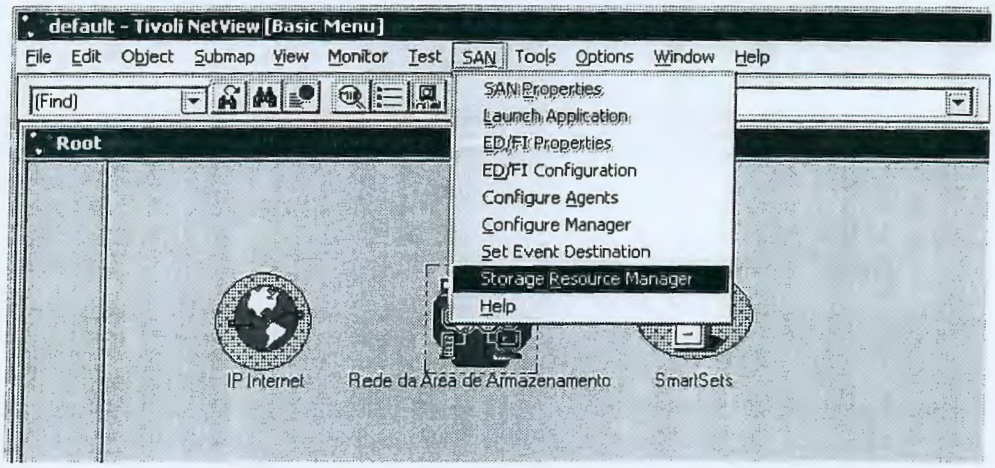


Figura 2. Iniciando o Tivoli Storage Resource Manager

Notas:

1. Se você utilizar o console remoto do Tivoli Storage Area Network Manager para ativar o IBM Tivoli Storage Resource Manager ou sua interface gráfica com o usuário, o seguinte erro será exibido se o Tivoli Storage Area Network Manager não estiver em execução no momento:

   ```
   Impossível Ativar
   ```

2. Se o IBM Tivoli Storage Resource Manager não estiver instalado ou o valor atual de SRMURL não especificar o nome de host correto do IBM Tivoli Storage Resource Manager, o navegador padrão da Web não localizará o URL e exibirá uma mensagem de erro.

   ```
   Impossível Ativar o Navegador da Web
   <SRMURL>
   ```


RQS nº 03/2005 CN
CPMI - CORREIOS
Fls. Nº 1455
Doc. 3698

10379
A.

Capítulo 3. Exibindo a Rede

Este capítulo fornece informações sobre as seguintes tarefas:

- Iniciando o Tivoli Storage Area Network Manager
- Configurando os agentes
- Planejando polling
- Configurando o destino de eventos
- Selecionando e interpretando exibições
- Utilizando cores para indicar o status do dispositivo

Alguns dispositivos de rede, como comutadores Fibre Channel, contêm aplicativos para ajudar no gerenciamento e na configuração desses dispositivos. Consulte o Capítulo 4, "Trabalhando com Recursos", na página 41 para obter informações sobre como iniciar aplicativos do dispositivo de rede.

Iniciando a Interface Gráfica com o Usuário do Tivoli Storage Area Network Manager

Para iniciar o Tivoli Storage Area Network Manager:

- Clique no ícone do Tivoli NetView, no desktop. O console do Tivoli NetView será exibido.
- Você pode acessar as funções do Tivoli Storage Area Network Manager a partir do menu **SAN**.

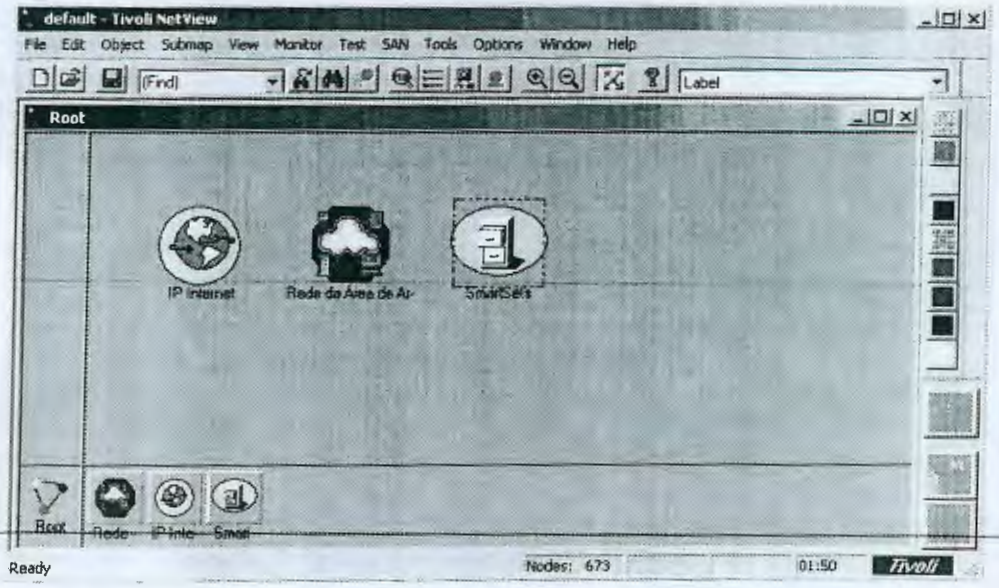


Figura 3. Iniciando a interface gráfica com o usuário do Tivoli Storage Area Network Manager

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI
Fls 1456
Doc 3698
15

Configurando os Agentes

O Tivoli Storage Area Network Manager utiliza agentes para descobrir sua SAN e monitorar o seu status. Utilizando o painel **Configuração do Agente** (consulte a Figura 4), você pode fazer o seguinte:

- Exibir ou remover agentes inativos na banda
- Exibir, incluir, remover ou configurar agentes fora da banda

Para acessar o painel **Configuração do Agente**, selecione **SAN → Configure Agents** no menu do console Tivoli NetView. A metade superior do painel mostra os **Agentes do IBM Tivoli Storage Area Network Manager** e a metade inferior mostra os **Agentes SNMP**.

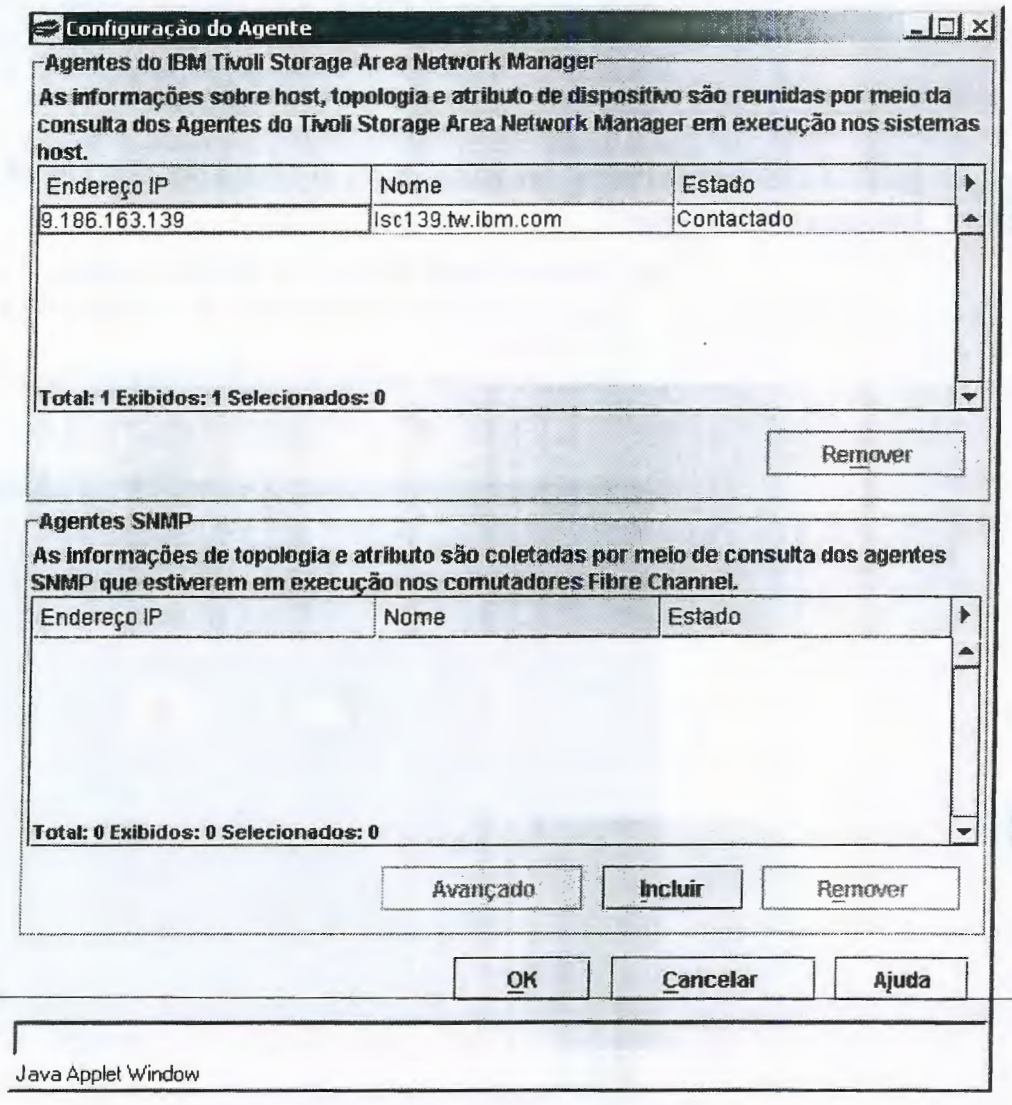


Figura 4. Painel Configuração do Agente

Agentes do IBM Tivoli Storage Area Network Manager

Esses agentes descobrem informações sobre cada sistema host gerenciado, seu armazenamento local e toda a SAN observável através da placa do barramento do host do sistema. As placas do barramento do host utilizam protocolos de descoberta em banda para reunir as informações. Esse painel

pode mostrar um agente em cada sistema de host gerenciado. Todos os agentes devem estar no estado **Contactado**. Consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* se tiver um sistema sem um agente.

Agentes SNMP

Se você não utilizar descoberta em banda, precisará configurar o Tivoli Storage Area Network Manager para tentar a descoberta fora da banda. A descoberta fora da banda utiliza consultas SNMP por meio de uma conexão TCP/IP para reunir informações sobre topologia e atributos. Consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* para obter informações adicionais sobre agentes SNMP.

Para configurar a descoberta fora da banda, faça o seguinte:

1. Clique no botão **Incluir**. O diálogo **Digite o Endereço IP ou o Nome** aparecerá (consulte Figura 5).

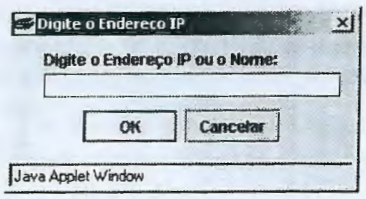


Figura 5. Configurar agente SNMP

2. Digite o endereço IP ou o nome da chave. Você pode digitar um nome completo, como **switchxm.rchland.ibm.com** ou um nome simples não qualificado, como **switchxm**.
3. **(Opcional)** O botão **Avançado** é somente para chaves Brocade. Clique no botão **Avançado** no painel de configuração do agente para definir o nome do usuário e a senha para a chave Brocade SNMP fora da banda. Isso permite que mais informações sejam reunidas a partir dos comutadores SNMP Brocade.

   Nota: É preciso inserir as informações de login para a conta Admin na chave Brocade. Nenhuma outra conta é suportada.

   Depois de digitar o ID do usuário e a senha e o próximo poll ser executado, verifique o log de mensagens para a seguinte mensagem:

   ```
   BTAQE1132E:  O ID do usuário ou a senha inseridos para o endereço
   de destino do agente fora da banda <endereço_do_destino>
   estão incorretos.
   ```

   Se você vir essa mensagem no log, insira novamente o ID de usuário e senha corretos.
4. Clique no botão **OK** para atualizar o painel (consulte a Figura 6 na página 18).

1037 A
RQS nº 03/2005 - CN
CRM
CORREIOS
FLS Nº 1457
Nº 3698
Doc.

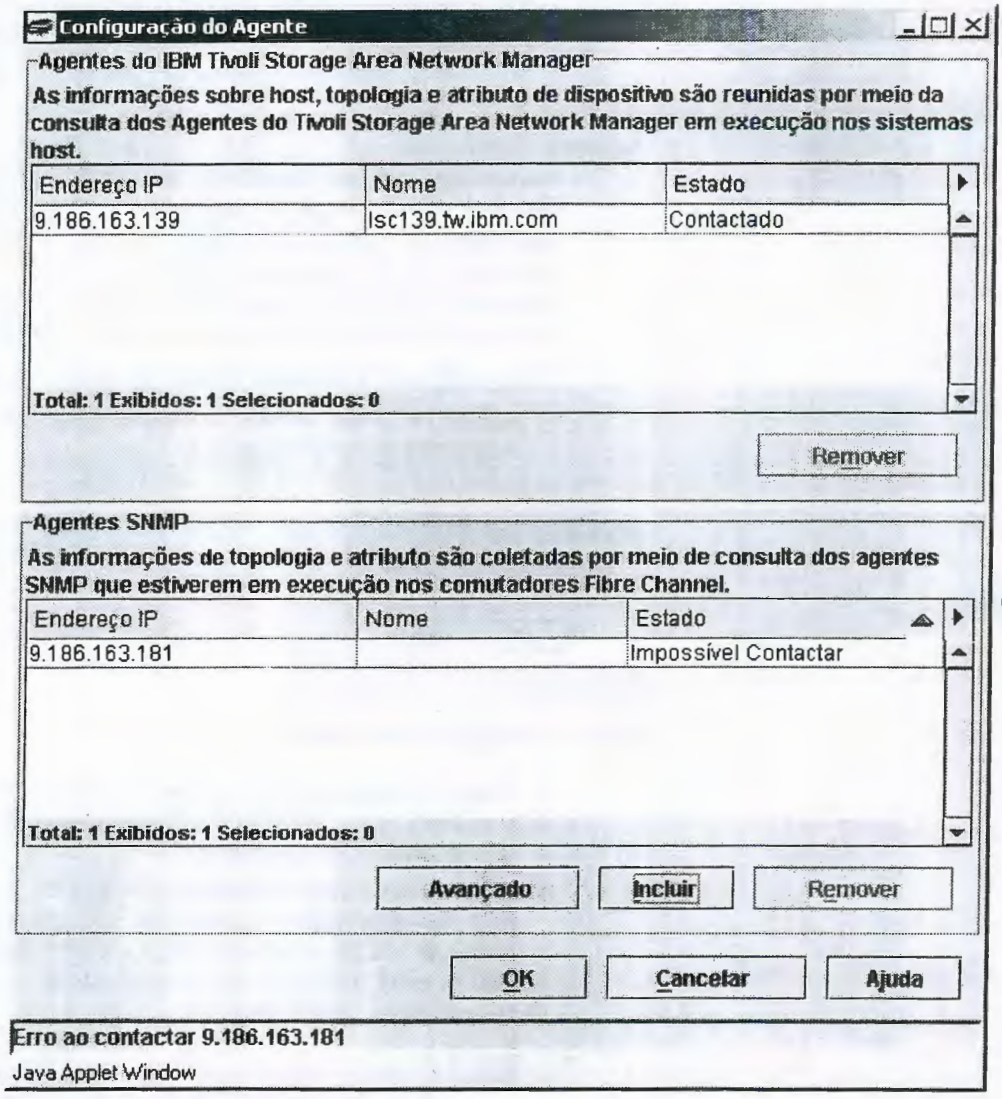


Figura 6. Configurar agente SNMP

Notas:

1. O campo **Estado** para o Agente SNMP na Figura 6 agora mostra que o Agente SNMP está **Contactado**. Se o estado **Contactado** não for exibido, verifique se o nome ou o endereço inserido está correto. Se o nome ou o endereço estiver correto, verifique se o comutador realmente suporta discovery fora da banda.
2. Se você desinstalar um agente e, em seguida, reinstalá-lo com um novo número de porta, após o discovery, serão exibidas duas ocorrências do agente no painel Agente de Configuração. O agente desinstalado mostrará o estado **Não Respondendo** e o agente instalado mostrará o estado **Contactado**. Para evitar confusão, remova o agente desinstalado do painel Agente de Configuração utilizando o botão **Remover**.

Você sabe se sua chave suporta descoberta em banda ou fora da banda?
O site do Tivoli na Web Tivoli http://www.ibm.com/software/support/ mostra o tipo de suporte para vários comutadores comuns. Entre em contato com o fornecedor do comutador se ele não estiver na lista.

10375
A-

Configurando o Destino de Eventos

O Tivoli NetView fornece um navegador de eventos para visualizar traps. É possível controlar e filtrar os eventos por meio da configuração dos dispositivos para enviar traps SNMP para o NetView e, em seguida, configurar o NetView para enviar traps SNMP para o Tivoli Storage Area Network Manager. O Tivoli Storage Area Network Manager executa uma descoberta quando ocorre um evento que atualiza o banco de dados.

Nem todos os traps que podem ser publicados por dispositivos indicam alterações no status da SAN ou na configuração. Por exemplo, muitos dispositivos suportam vários níveis de traps SNMP e a monitoração de parâmetros e contadores internos. Esses traps causariam muitas redescobertas não desejadas pelo Tivoli Storage Area Network Manager. Somente eventos que indiquem uma alteração na SAN ou na configuração devem ser encaminhados ao Tivoli Storage Area Network Manager. Se você tiver outros MIBs proprietários de chaves e dispositivos de armazenamento que indiquem alterações de status ou de configuração, esses eventos também devem ser encaminhados ao Tivoli Storage Area Network Manager. Por exemplo, eventos de um Enterprise Storage Server que indicam alterações internas, tais como alterações de configuração de LUN, devem ser encaminhados ao Tivoli Storage Area Network Manager para que uma descoberta seja iniciada.

Para obter informações de configuração sobre o encaminhamento de traps para o NetView e o Tivoli Storage Area Network Manager, consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

Você pode utilizar o Tivoli NetView Event Browser para exibir eventos no banco de dados de eventos do Tivoli NetView. Consulte "Utilizando SNMP para Gerenciar Eventos" na página 43 para obter mais informações.

Para utilizar o Tivoli NetView Event Browser dessa maneira, utilize o painel **Definir Destino do Evento** para configurar o destino dos traps do SNMP e dos eventos TEC, da seguinte maneira:

1. Clique no ícone do Tivoli NetView, no desktop. O console do Tivoli NetView será exibido.
2. Selecione **SAN → Definir Destino do Evento** no console do Tivoli NetView. A janela Definir Destino de Evento é exibida.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1458
Nº Doc. 3698

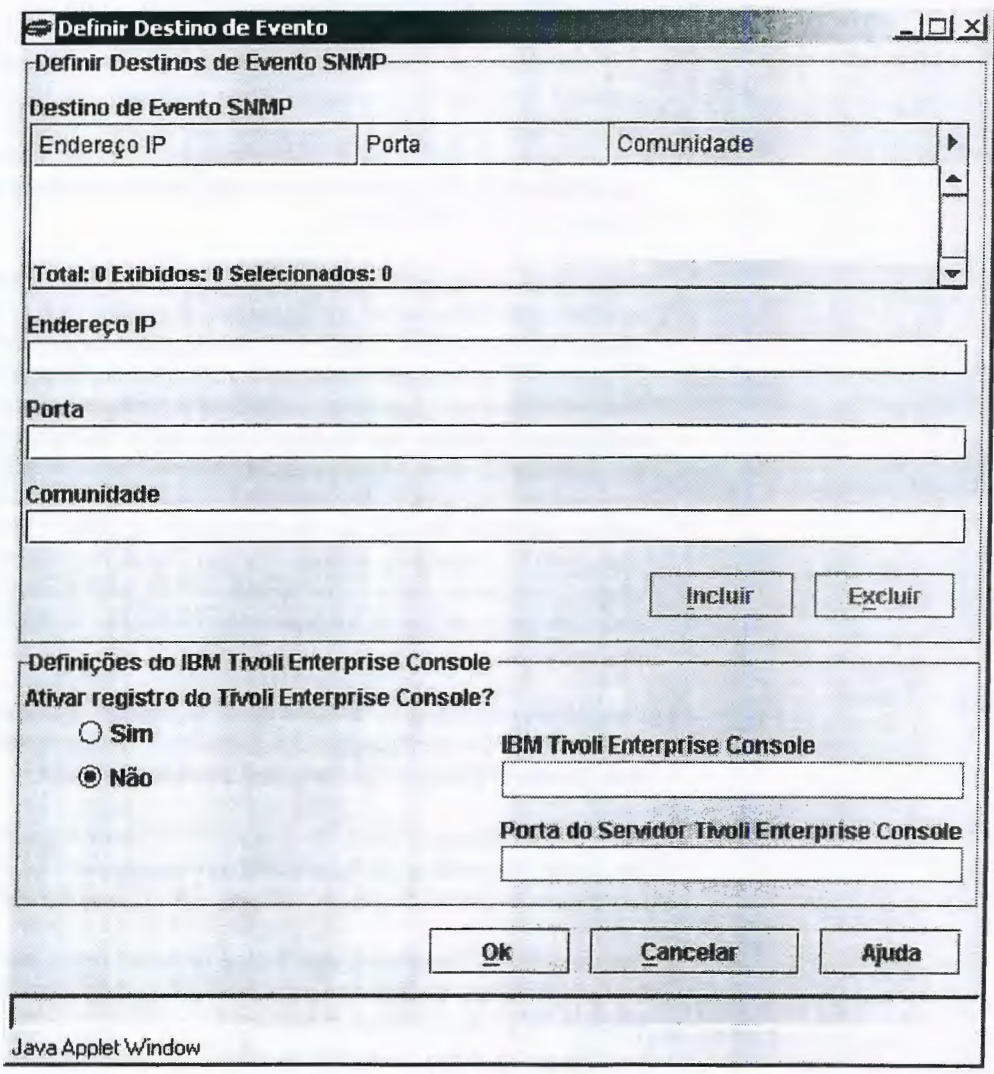


Figura 7. Definir Destino de Evento

O primeiro campo do painel permite que você defina o destino de evento do SNMP. Quando você digita um Endereço IP, uma Porta e uma Comunidade, os botões **Incluir** e **Excluir** são ativados. Os campos que podem ser definidos são os seguintes:

Endereço IP
O endereço IP de um host ou um dispositivo que pode receber traps do SNMP.

Porta O número da porta que o host ou o dispositivo utilizará para atender traps do SNMP. O padrão é **162**.

Comunidade
O nome da comunidade à qual o host ou o dispositivo do SNMP é atribuído. O padrão é **Público**.

Utilize o botão **Incluir** para incluir um destino de evento SNMP ao quadro de listagem, na parte superior. Utilize o botão **Excluir** para excluir um destino de evento SNMP da lista.

Se você selecionar **Sim** para ativar o registro em log do Tivoli Enterprise Console, poderá inserir informações nestes campos:

IBM Tivoli Enterprise Console
Esse é o endereço IP do seu servidor Tivoli Enterprise Console. Ele será obrigatório se você estiver utilizando o Tivoli Enterprise Console.

Porta do Servidor Tivoli Enterprise Console
Esse é o número da porta do seu servidor Tivoli Enterprise Console. Ele será obrigatório se você estiver utilizando o Tivoli Enterprise Console.

3. Insira as informações apropriadas na janela Definir Destino de Evento e clique no botão **Ok**.

Planejando Polling

Quando você iniciar o Tivoli Storage Area Network Manager, ele descobrirá os dispositivos em sua SAN fazendo o polling dos agentes. Para planejar o polling, execute as seguintes etapas:

1. Selecione **SAN → Configure Manager**, no console do Tivoli NetView. Isso exibe o painel **Configuração da SAN**, mostrado na Figura 8.

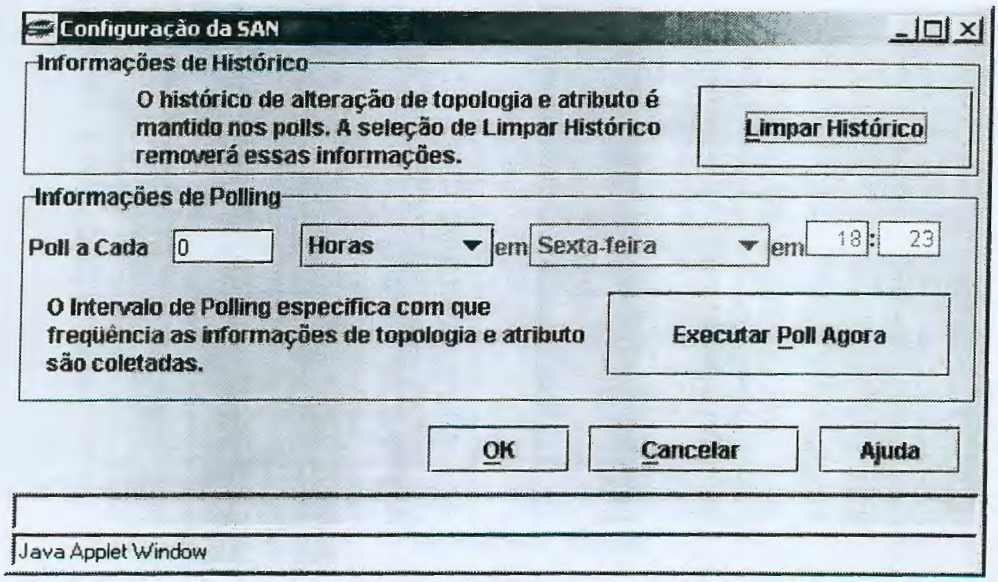


Figura 8. Painel Configuração da SAN

   - Para fazer o poll de informações da SAN imediatamente, clique no botão **Executar Poll Agora**.
   - Para planejar o polling em uma data e hora específicas, faça as seleções apropriadas na seção de informações de polling.
   - Para parar o polling planejado, insira **0** no campo **Poll a Cada**.
2. Clique no botão **OK**.

Considerações:

- Utilize o botão **Limpar Histórico** para atualizar as informações de polling reunidas anteriormente. Por exemplo, se um dispositivo for relatado como ausente por não ser mais detectado, a limpeza do histórico irá removê-lo do console. Consulte "Limpando o Histórico de Status" na página 36 para obter mais informações.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1459
3698
Doc.

- O tempo necessário para concluir o polling depende do tamanho de sua SAN.

Exibindo a Ajuda On-line

Você pode exibir a ajuda on-line da seguinte maneira:
- Selecione o menu **Ajuda** na maioria das janelas.
- Clique no ponto de interrogação (?) exibido no Assistente de Tarefas.
- Clique no botão **Ajuda** na maioria das janelas.

Selecionando e Interpretando Exibições da Rede

Quando o Tivoli NetView é iniciado, ele exibe o submapa raiz, consulte a Figura 9. Os símbolos **IP Internet** e **SmartSets** são símbolos padrão do NetView para submapas com base em IP.

O símbolo **Rede da Área de Armazenamento** representa o submapa da Rede de Armazenamento.

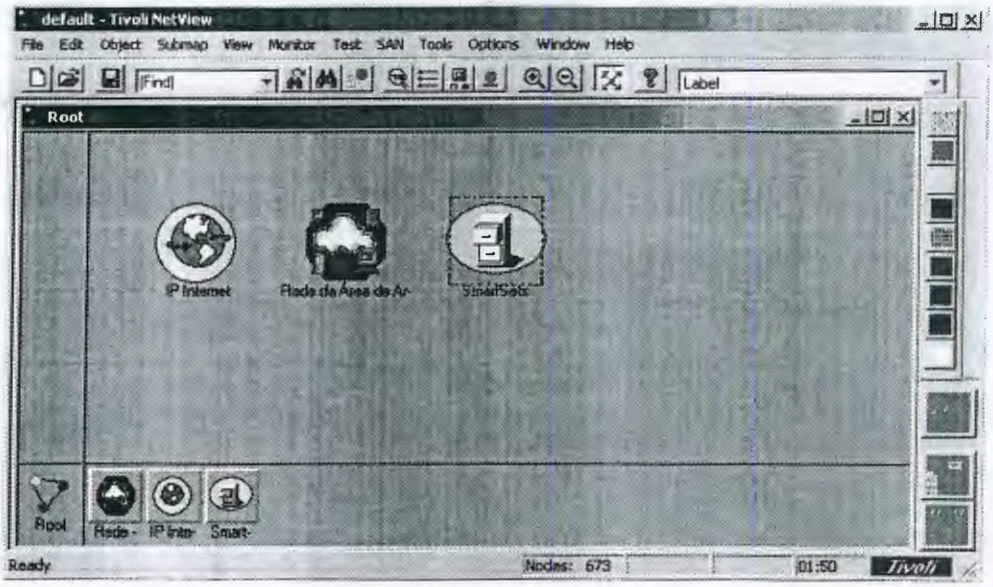


Figura 9. Submapa raiz

Para exibir graficamente sua Rede da Área de Armazenamento, dê um clique duplo no símbolo **Rede da Área de Armazenamento**.

Se você preferir exibir a rede na exibição de exploração do submapa, selecione **Window → Submap Explorer**, no menu do console do NetView.

Para ver a exibição gráfica e a exibição de exploração, selecione **Window → Tile Horizontally**, no menu do console do NetView.

A Figura 10 na página 23 mostra o submapa das redes de área de armazenamento. Para ver esse submapa, dê um clique duplo no símbolo **Rede da Área de Armazenamento** na Figura 9.

10371
A.

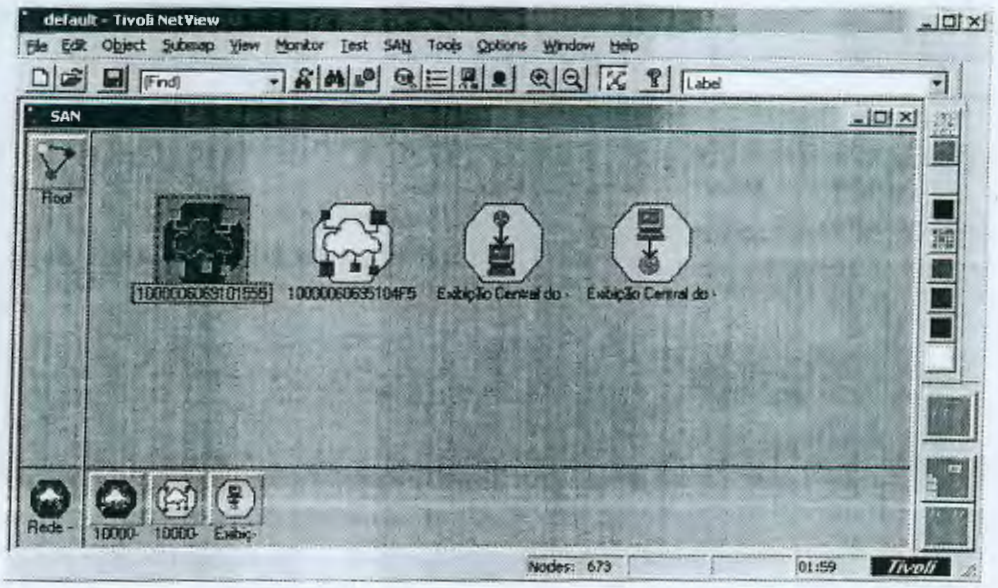


Figura 10. Rede da Área de Armazenamento

O submapa da Rede da Área de Armazenamento (Figura 10) contém símbolos para o seguinte:

Símbolos da SAN
Você verá um símbolo para cada SAN. Se você clicar em um símbolo da SAN, começará a explorar aquela SAN. Este gráfico também mostra um exemplo das dicas de propriedades, que você pode obter se mantiver o ponteiro do mouse sobre um símbolo por alguns segundos.

Símbolo da Exibição Central do Dispositivo
Você pode ter várias SANs com diversos dispositivos de armazenamento. A **Exibição Central do Dispositivo** permite que você veja todos os dispositivos de armazenamento e suas relações lógicas (potenciais) com todos os hosts. Essa exibição não mostra os comutadores ou outros dispositivos de conexão. Dê um clique duplo no símbolo **Exibição Central do Dispositivo** para exibir o seu submapa. A exibição central do dispositivo não é preenchida com o discovery fora da banda. A exibição central do dispositivo requer agentes na banda para reunir as informações.

Símbolo da Exibição Central do Dispositivo
Você pode ter várias SANs com diversos sistemas host. A **Exibição Central do Host** permite que você veja todos os sistemas host e sua relações lógicas com os dispositivos de armazenamento locais e conectados à SAN. Dê um clique duplo no símbolo **Exibição Central do Host** para exibir o seu submapa. A exibição central do host não é preenchida com o discovery fora da banda. A exibição central do host requer agentes na banda para reunir as informações.

Exibição da SAN

Dê um clique duplo em um símbolo da SAN para exibir o seu submapa; consulte a Figura 11 na página 24. Observe que você pode optar por uma **Exibição da Topologia** ou uma **Exibição das Zonas** da SAN. A Exibição da Topologia mostra a SAN inteira enquanto a Exibição das Zonas mostra a SAN como um agrupamento de zonas. Dê um clique duplo no símbolo da exibição desejada.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 1460
Doc. 3698

Figura 11. Exibição da SAN

Exibição da Topologia

A exibição da topologia (Figura 12) apresenta dois tipos de símbolos:

- Um símbolo (no centro) representa todos os elementos de conexão da SAN.
- Um símbolo para cada segmento, em que um segmento consiste em um comutador e os dispositivos conectados diretamente a ele.

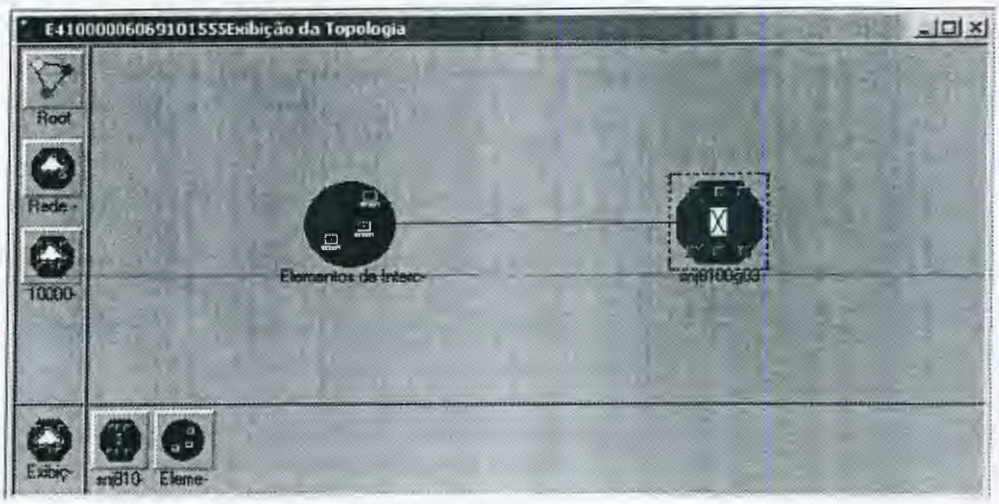


Figura 12. Exibição da Topologia

Dar um clique duplo em um segmento exibe o conteúdo desse segmento. Veja os resultados na Figura 13 na página 25.

10369
A-

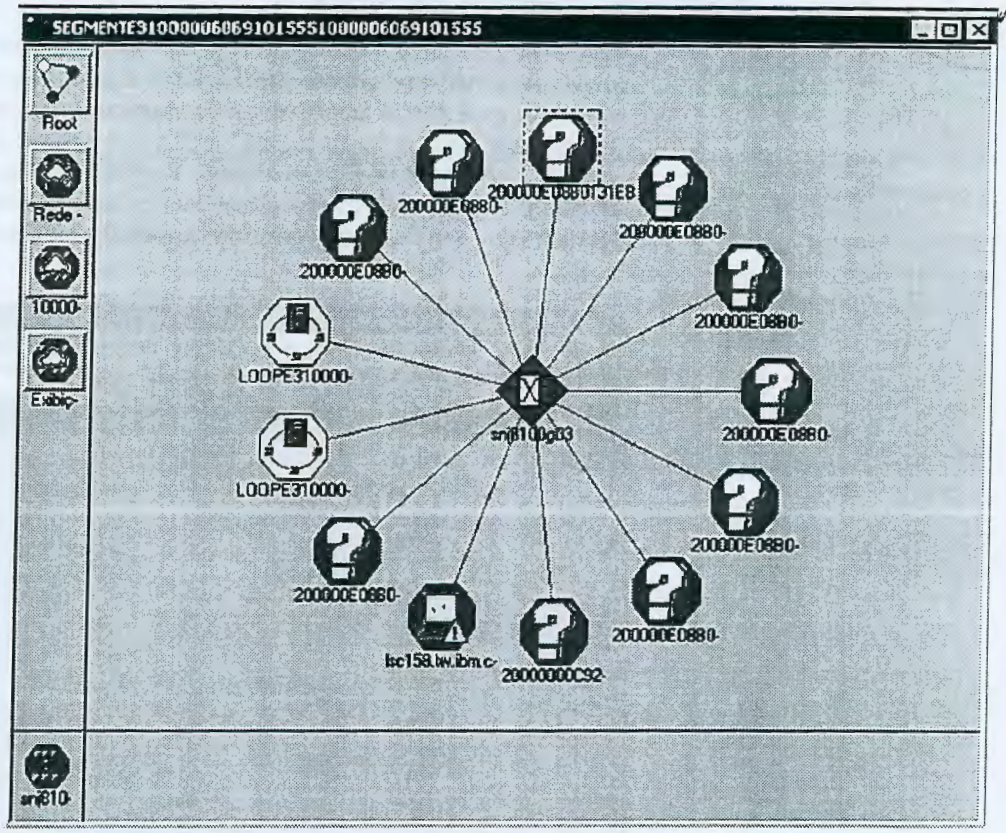


Figura 13. Exibição do segmento

A exibição mostrada na Figura 13 pode mostrar conexões para sistemas host gerenciados, sistemas host não gerenciados, chaves, gabinetes do disco, etc. Um host não gerenciado não tem um agente do Tivoli Storage Area Network Manager sendo executado nele.

Nesta seção, seguimos um caminho por meio da topologia da rede. A qualquer momento, você poderá seguir outro caminho clicando em um dos símbolos na pilha de submapas.

Exibição das Zonas

Se sua SAN contiver chaves que suportam os padrões de zoneamento GS-3 Fibre Channel ou se você tiver definido o nome do usuário e a senha para descobertas fora de banda para chaves Brocade no painel Configuração do Agente (consulte "Configurando os Agentes" na página 16), o Tivoli Storage Area Network Manager recuperará e exibirá as zonas configuradas. Para selecionar a Exibição das Zonas, dê um clique duplo no símbolo **Exibição das Zonas**, mostrado na Figura 11 na página 24. Isso exibirá um símbolo para cada zona descoberta.

Você não tem certeza de que o seu comutador suporta os padrões de zoneamento GS-3 Fibre Channel?

O site do Tivoli na Web http://www.ibm.com/software/support/ mostra o suporte mais recente para vários comutadores comuns. Se o seu comutador não suportar os padrões de zoneamento GS-3, ainda assim você poderá exibir informações sobre o zoneamento, iniciando um aplicativo do comutador (consulte o "Iniciando Aplicativos de Dispositivos de Rede" na página 41).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1461
3698
Doc

Exibição Central do Host

A exibição central do host apresenta a relação entre os sistemas host e o seu armazenamento local e conectado à SAN. Essa é uma *exibição lógica*, pois os comutadores e outros dispositivos de conexão intervenientes não são mostrados. Como essa é uma exibição lógica, você pode preferir observar essa relação com a exploração do submapa. Para acessar a exibição central do host da exploração do submapa, clique com o botão direito do mouse no símbolo **Exibição Central do Host** e clique em **Explore**, conforme mostrado na Figura 14.

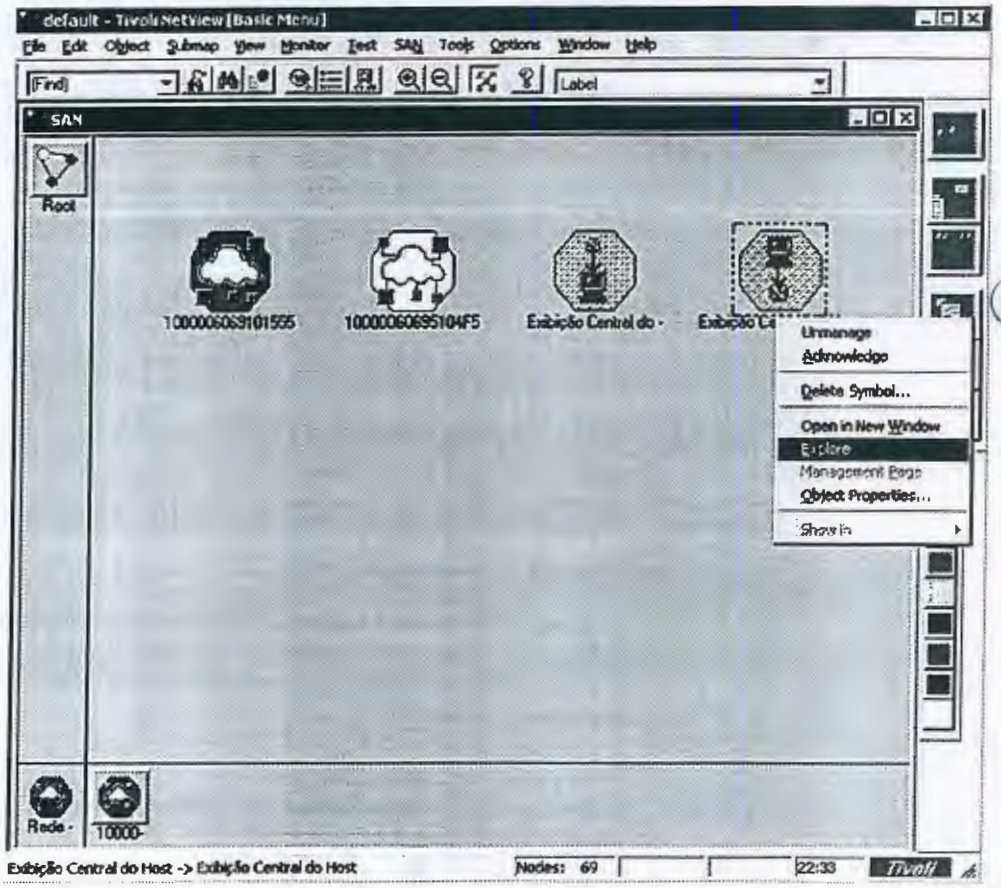


Figura 14. Exibição de exploração central do host

A exibição de exploração central do host é mostrada na Figura 15 na página 27. O painel direito mostra que existem três sistemas hosts.

10367
A.

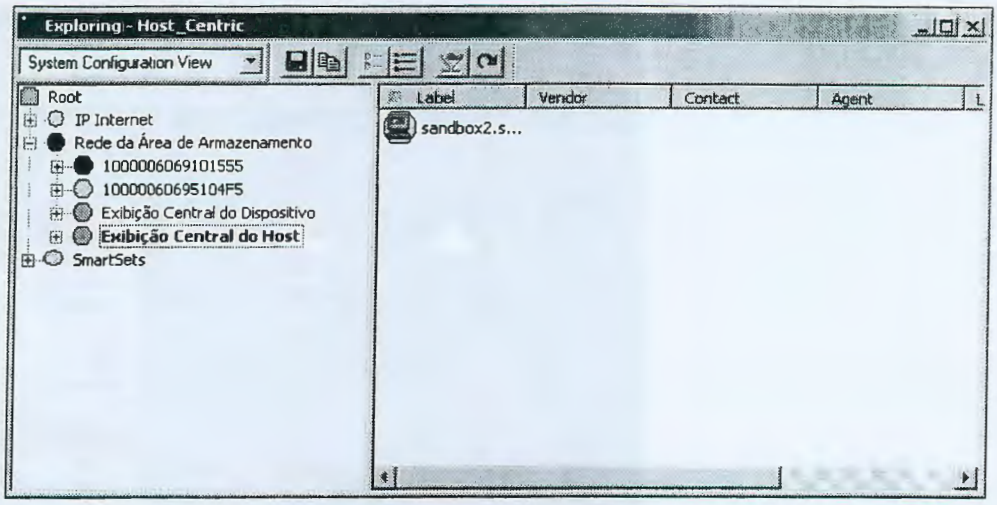


Figura 15. Exibição central do host — hosts

Nota: Na primeira vez que o gerenciador for iniciado, uma descoberta de topologia será executada, de modo que as exibições centrais no dispositivo e no host não serão atualizadas. Você pode atualizar essas exibições, executando um poll agora. Consulte "Planejando Polling" na página 21 para obter mais informações.

Expanda o símbolo da **Exibição Central do Host**. Você pode navegar para um sistema operacional do host e para os sistemas de arquivos da seguinte maneira:

- Dê um clique duplo em um símbolo do host para exibir o sistema operacional do host.
- Dê um clique duplo no símbolo do sistema operacional para exibir os sistemas de arquivos.
- Dê um clique duplo no símbolo **HostFileSys:**, no painel à direita, para exibir os volumes lógicos.
- Clique no símbolo **Volume Lógico:**, no painel à direita, para exibir o dispositivo de armazenamento em disco.

Exibição Central do Dispositivo

A exibição central do dispositivo apresenta a relação lógica entre os dispositivos de armazenamento e os sistemas host. Essa exibição é chamada de *exibição lógica*, pois os comutadores ou outros dispositivos de conexão intervenientes não são mostrados. Como essa é uma exibição lógica, você pode preferir exibi-la utilizando a exploração do submapa. Para selecionar a exibição central do dispositivo da exploração do submapa, clique com o botão direito do mouse no símbolo **Exibição Central do Dispositivo** e clique em **Explore**, conforme mostrado na Figura 16 na página 28.

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 1462
Nº 3698
Doc

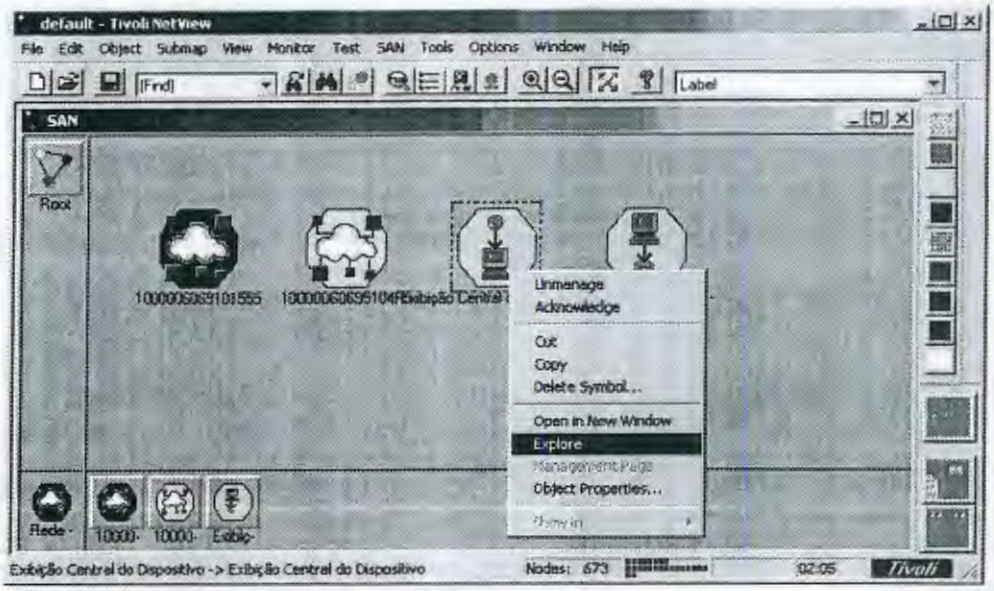


Figura 16. Exibição de exploração central do dispositivo

Conforme mostrado na Figura 17, essa exibição contém um símbolo para cada dispositivo de armazenamento.

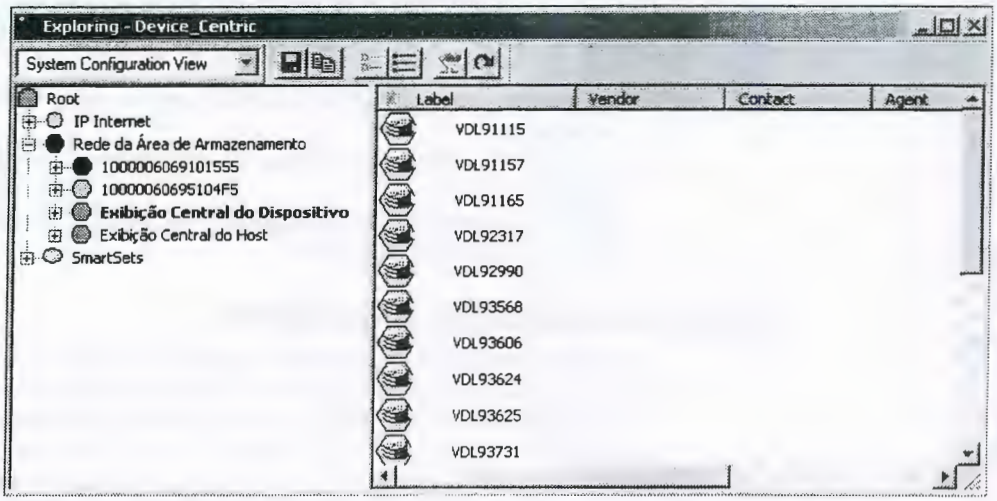


Figura 17. Exibição central do dispositivo

Nota: Na primeira vez que o gerenciador for iniciado, uma descoberta de topologia será executada, de modo que as exibições centrais no dispositivo e no host não serão atualizadas. Você pode atualizar essas exibições, executando um poll agora. Consulte "Planejando Polling" na página 21 para obter mais informações.

Expanda o símbolo da **Exibição Central do Dispositivo**. Você pode navegar para dispositivos e LUNs associadas, hosts, sistemas operacionais e sistemas de arquivos, da seguinte maneira:

- Dê um clique duplo em um dos símbolos de **Disco**, no painel à direita, para exibir as LUNs associadas.
- Dê um clique duplo em um dos símbolos da **LUN**, no painel à direita, para exibir os hosts associados.

10365
A

- Dê um clique duplo no símbolo do host, no painel à direita, para exibir o sistema operacional.
- Dê um clique duplo no símbolo do sistema operacional, no painel á direita, para exibir os sistemas de arquivos.

Exibindo as Propriedades do Dispositivo da SAN

O Tivoli Storage Area Network Manager armazena as informações que ele descobre sobre os dispositivos na SAN. Para acessar essas informações, clique no símbolo do dispositivo no submapa e selecione **SAN → SAN Properties** no menu do console. A Figura 18 mostra como selecionar as propriedades de uma chave Fibre Channel denominada **SRMSW4**.

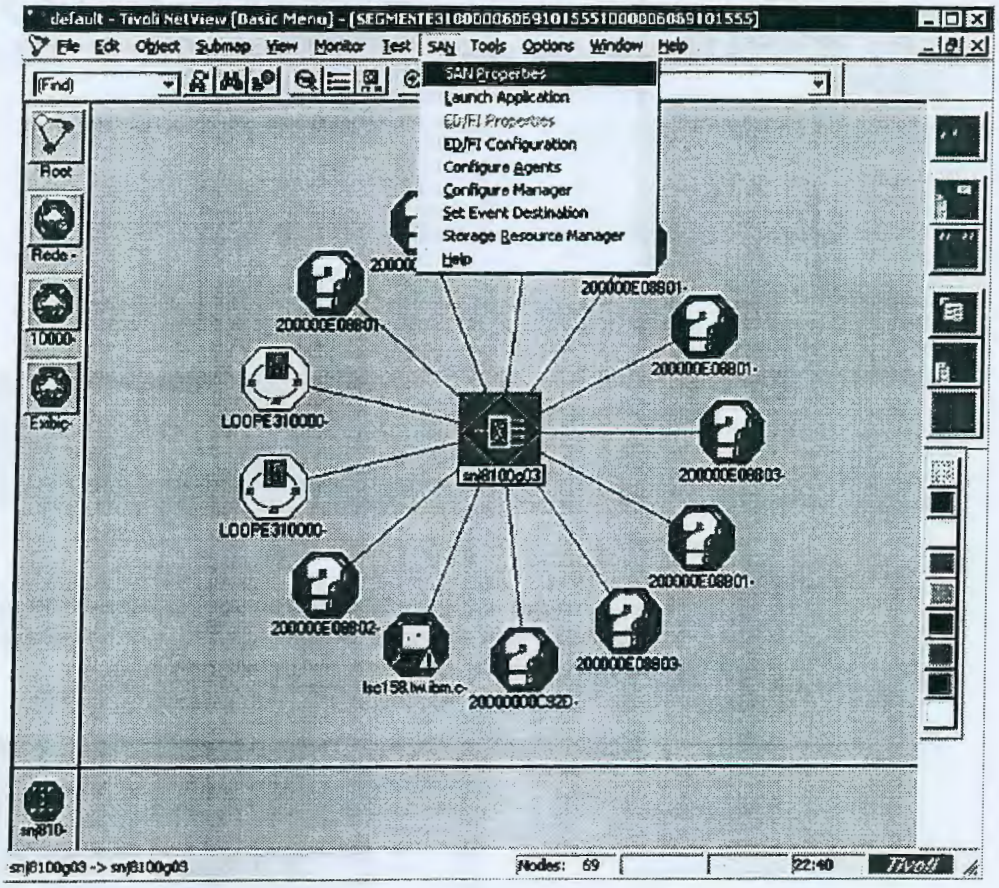


Figura 18. Exibindo propriedades do dispositivo da SAN

A Figura 19 na página 30 mostra as propriedades do comutador. Se você selecionou um dispositivo de armazenamento, veria as propriedades exclusivas desse dispositivo de armazenamento. Para obter informações detalhadas sobre os campos de propriedades exibidos, clique no botão **Ajuda**, no canto inferior direito da exibição de propriedades.

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 1463
3698
Doc.

10364
A.

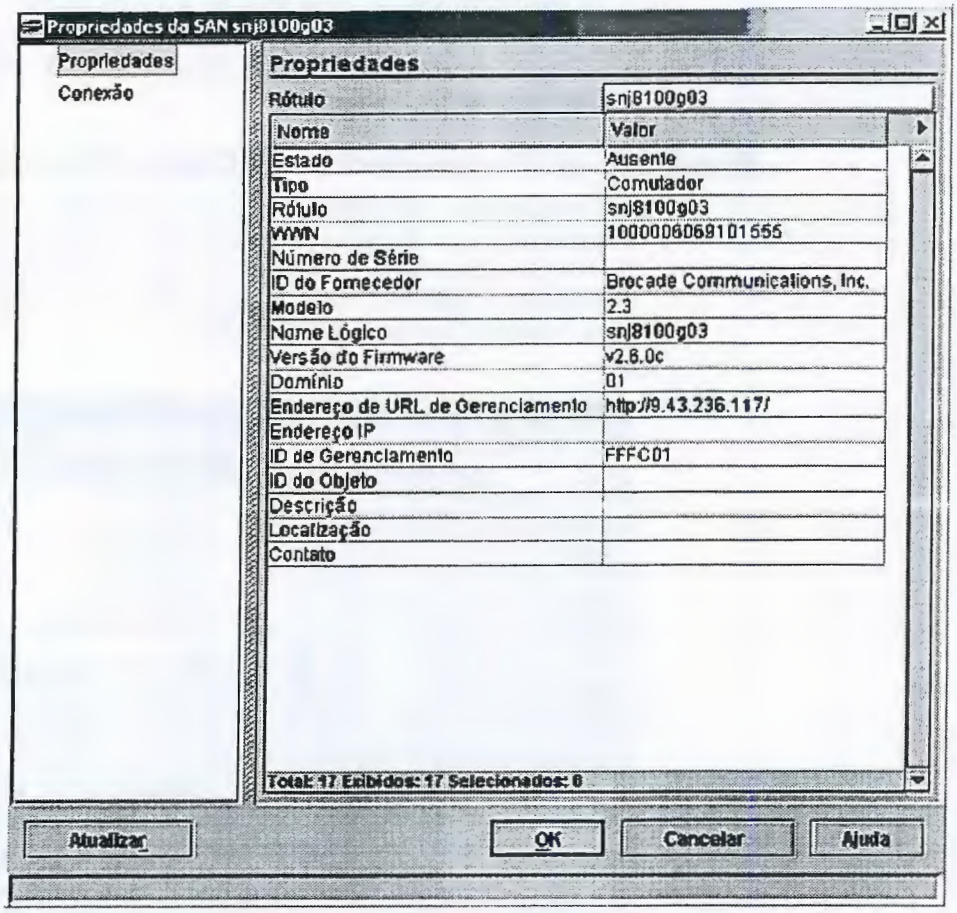


Figura 19. Exibição de Propriedade

Observe que a Figura 19 também contém uma opção de **Conexão**, no painel à esquerda. Para exibir informações sobre a conexão desse comutador, clique na opção **Conexão**, conforme mostrado na Figura 20.

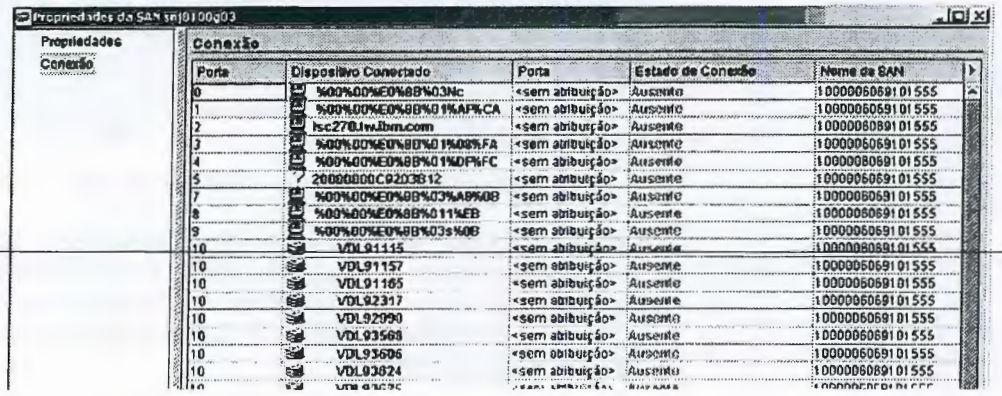


Figura 20. Exibição de Conexão

Se o dispositivo selecionado for um comutador de rede que fornece dados do sensor e de eventos para o Tivoli Storage Area Network Manager, você poderá clicar na opção **Sensores/Eventos** (Figura 21 na página 31) para exibir informações

10363

sobre o sensor a partir do dispositivo e listar os eventos relatados pelo dispositivo em resposta a uma consulta no dispositivo.

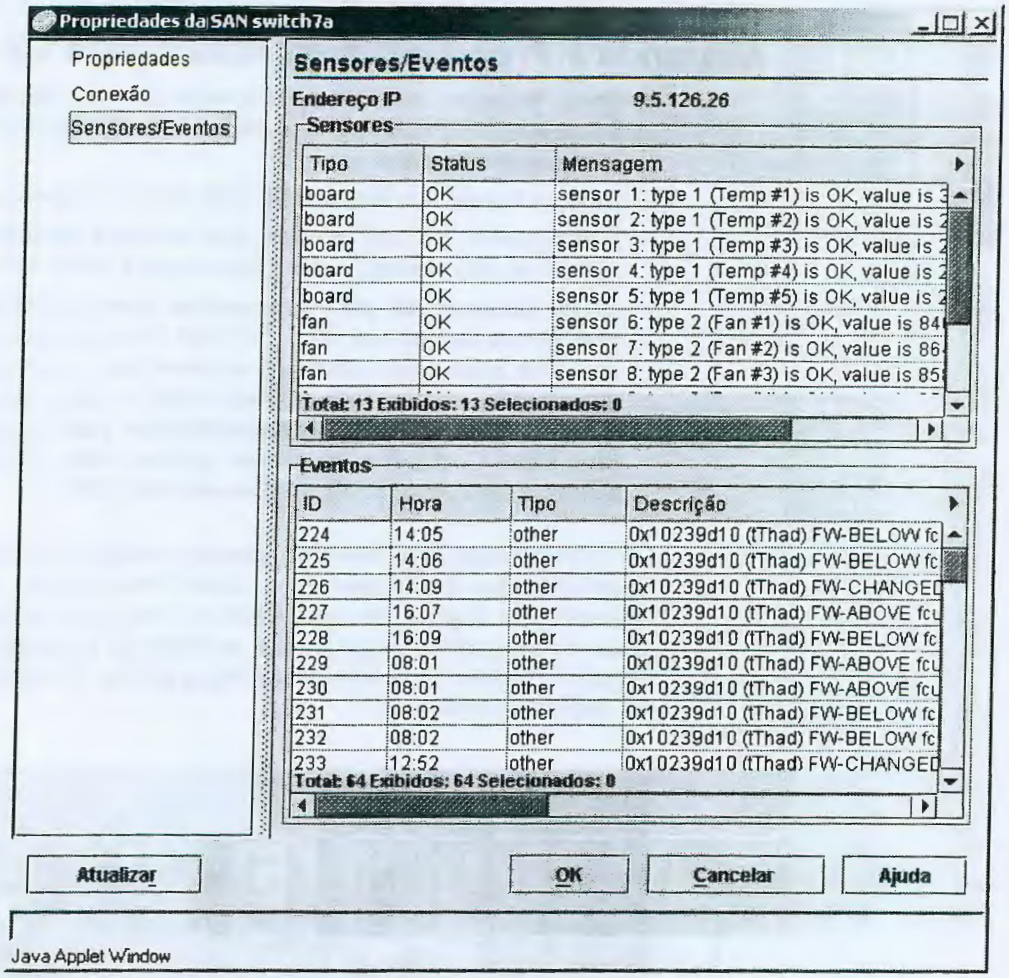


Figura 21. Exibição Sensores/Eventos

Clique no botão **Ajuda** para obter uma explicação detalhada de todos os campos nessas exibições. Por exemplo, o campo **Estado** controla o Status, conforme descrito na tabela a seguir.

Tabela 3. Estados da conexão

Estado	Significado	Status
Normal	Limpar Histórico foi executado em um Novo dispositivo.	Normal
Ausente	Dispositivo detectado anteriormente não é mais detectado. Limpar Histórico remove esse dispositivo de todos os submapas e todas as exibições.	Crítico
Atributo Modificado	Um ou mais atributos foram alterados. Limpar Histórico altera o estado para Normal.	Normal

Por padrão, o Tivoli NetView coleta informações sobre todos os dispositivos que podem ser afetados pelas conexões TCP/IP. Por exemplo, se você tiver um comutador Fibre Channel que também suporte uma conexão TCP/IP, o Tivoli NetView utilizará o TCP/IP para reunir informações sobre esse comutador. Para

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1464
Nº 3698
Doc.

exibir essas informações, clique com o botão direito do mouse em um símbolo de dispositivo no console do Tivoli NetView e clique em **Object Properties**, no menu de contexto resultante. Observe que essas informações serão menos precisas do que as informações reunidas pelo Tivoli Storage Area Network Manager.

Alterando a Propriedade do Rótulo para um Símbolo

O Tivoli Storage Area Network Manager permite alterar os rótulos e os ícones de determinados dispositivos na exibição da topologia do Tivoli NetView. Isso resulta nos seguintes benefícios:

- Ajuda a tornar a exibição mais fácil de ler e entender.
- É útil quando o Tivoli Storage Area Network Manager detecta um dispositivo de rede, mas não consegue obter informações sobre esse dispositivo.
- É especialmente útil para implementar uma estratégia de agente bem colocada para gerenciamento da SAN. O Tivoli Storage Area Network Manager permite que você especifique informações sobre hosts conectados Fibre Channel que são descobertos, mesmo quando você optar por não implementar um agente nesses hosts. Você pode utilizar essa flexibilidade para executar o Gerenciamento da SAN Fibre Channel de hosts sem agentes, além de empregar uma estratégia bem colocada de agente de Gerenciamento da SAN.

O Tivoli Storage Area Network Manager rotula o dispositivo como **desconhecido** e representa esse dispositivo com o ícone Desconhecido, utilizando o WWN (nome mundial) do dispositivo como o rótulo. Você pode aplicar os seus próprios rótulo e ícone ao dispositivo para tornar a exibição da topologia mais significativa. A Figura 22 mostra uma tela de topologia parcial Tivoli NetView com vários objetos de rede desconhecidos.

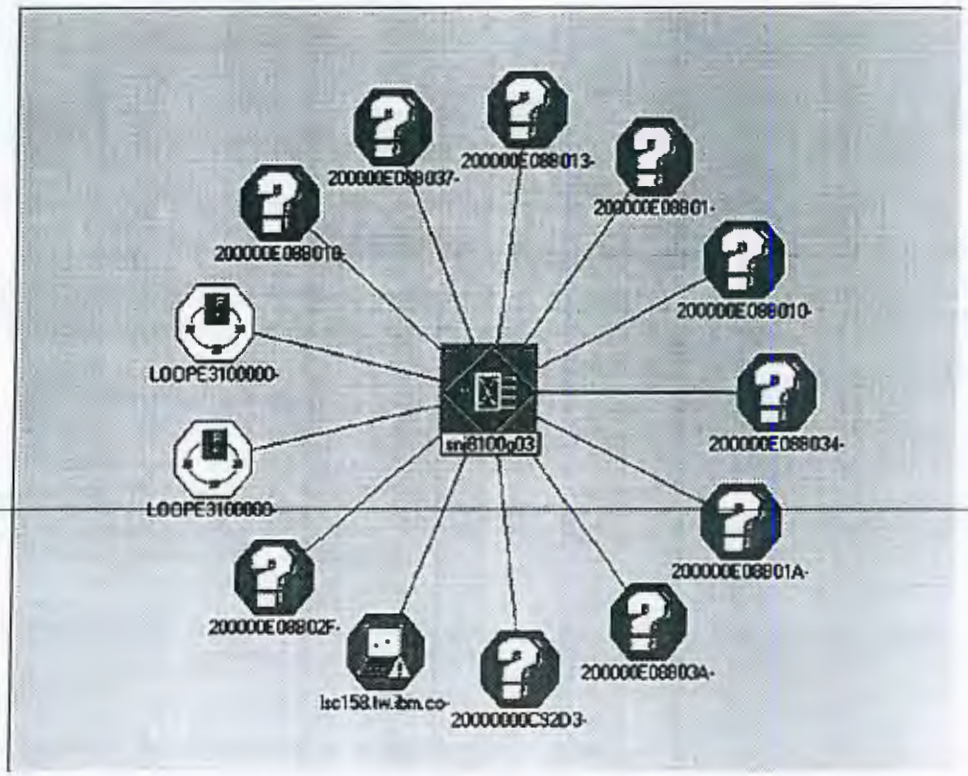


Figura 22. Tela de topologia parcial mostrando objetos desconhecidos

Para alterar o rótulo e o ícone de um dispositivo desconhecido, execute as seguintes etapas:

1. Clique no dispositivo a ser modificado e selecione **SAN → SAN Properties**, na barra de menus. A janela Propriedades é exibida.
2. Realce o campo Label e insira o novo rótulo desse dispositivo.
3. Para alterar o ícone desse dispositivo, abra a lista drop-down Icon e selecione um ícone na lista (Figura 23).

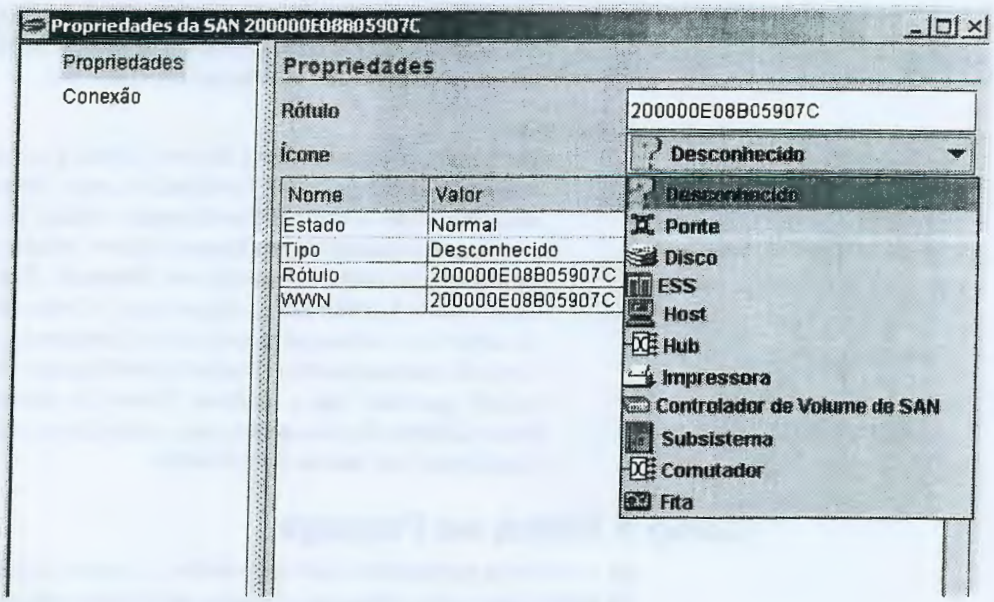


Figura 23. Lista drop-down Icon

4. Clique em **OK** para salvar as alterações e fechar a janela Propriedades. O rótulo e o ícone novos serão exibidos na tela de topologia do Tivoli NetView.

Compreendendo o Status

A cor do símbolo reflete o seu status. Por exemplo, a cor verde indica operação normal. A cor vermelha indica uma falha crítica. Consulte a Tabela 4 para obter as atribuições de cores.

Tabela 4. Status do Símbolo

Status	Significado do Status	Cor do Símbolo	Cor da Conexão
Desconhecido	Status não determinado.	Azul	Preto
Normal	Estado operacional normal.	Verde	Preto
Marginal	Danificado, mas ainda funcional.	Amarelo	Amarelo
Crítico	Sem funcionamento ou ausente.	Vermelho	Vermelho
Não gerenciado	Não monitorado. Veja a explicação a seguir.	Trigo (castanho)	Preto
Confirmado	Não monitorado. Veja a explicação a seguir.	Verde escuro	Preto

RQS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1465
Doc. 3698

Não gerenciado

Os objetos não gerenciados não são monitorados quanto a alterações na topologia e status, como são os objetos gerenciados. Uma cor é atribuída a um símbolo do objeto gerenciado de acordo com o seu status. Esse status se propaga até a árvore do submapa. Para parar o gerenciamento de um objeto, clique com o botão direito do mouse em seu símbolo no submapa e selecione **Não Gerenciar**, no menu de contexto. O símbolo será alterado para a cor dos objetos não gerenciados e permanecerá nessa cor até que o objeto seja gerenciado novamente. Para iniciar o gerenciamento do objeto novamente, clique com o botão direito do mouse em seu símbolo e selecione **Gerenciar**, no menu de contexto.

Confirmado

Você pode alterar o status de um objeto para **confirmado**, enquanto determina por que ele foi relatado como **crítico**, **marginal** ou **desconhecido**. O status **Confirmado** indica o reconhecimento de um problema enquanto o problema estiver sendo resolvido ou enquanto estiver pesquisando outro status de seu interesse. Para alterar o status de um objeto para **Confirmado**, clique com o botão direito do mouse no símbolo do objeto no submapa e selecione **Confirmar**, no menu de contexto. Um símbolo permanecerá no estado confirmado até que outro problema ocorra ou até que você *não o confirme*. Para não confirmar um objeto, clique com o botão direito do mouse em seu símbolo no submapa e selecione **Não Confirmar**, no menu de contexto.

Como o Status se Propaga

Se o símbolo representar um dispositivo, o status mostrado será o do dispositivo. Se representar um submapa, o status mostrado refletirá o status de um submapa filho e nenhum dos submapas abaixo desse submapa filho. A Tabela 5 mostra as regras padrão utilizadas para propagar o status até os submapas filho.

Nota: Quando você remover um dispositivo, a exibição da topologia será sempre atualizada. No entanto, as exibições centrais no host e no dispositivo nem sempre são atualizadas. Você pode atualizar as exibições centrais no host e no dispositivo, selecionando **SAN → Configure Manager** a partir do console do the Tivoli NetView e planejar o polling ou clicar no botão **Executar Poll Agora**.

Tabela 5. Propagação do Status Padrão

Status do Objeto	Condição de Símbolos no Submapa Filho
Desconhecido	Nenhum símbolo com status normal, crítico, marginal ou não gerenciado.
Normal	Todos os símbolos são normal ou confirmado.
Marginal	Um dos seguintes: • Todos os símbolos são marginais • Símbolos normais e marginais • Símbolos normal, marginal e crítico
Crítico	Pelo menos um símbolo é crítico e nenhum é normal.

10359
A.

Status na Exibição Gráfica do Submapa

Consulte a Figura 24 para obter um exemplo de status de símbolo na exibição gráfica. Se a opção de dicas de propriedade (no canto superior direito da exibição) for **Status**, conforme mostrado aqui, o status será exibido na barra de status (na parte inferior da exibição) e na dica de propriedade que é exibida quando você mantém o cursor em um símbolo do objeto. Além disso, se você posicionar o cursor sobre um dos botões de cores da barra de ferramentas do filtro de status, o significado daquela cor será exibido.

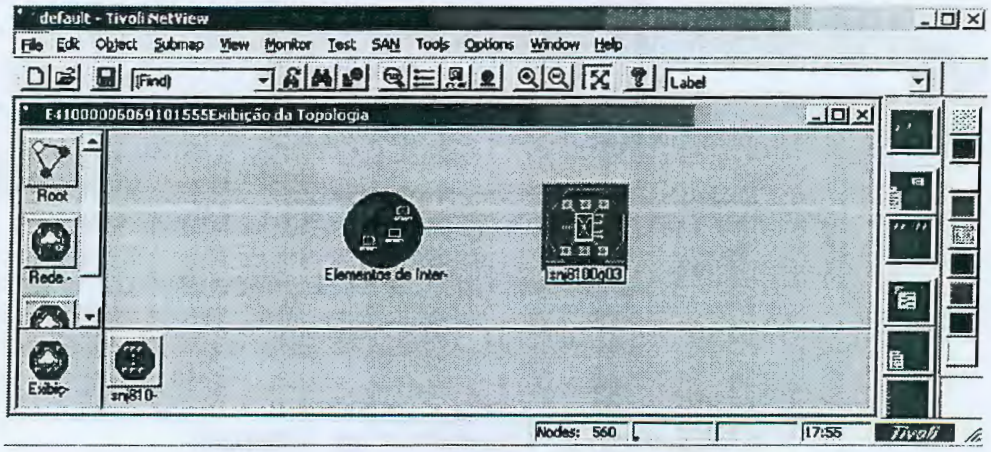


Figura 24. Status na exibição gráfica do submapa

Se sua opção de dicas de propriedade não estiver definida como **Status**, você poderá selecioná-la na lista drop-down de dicas de propriedade.

Status na Exibição de Exploração do Submapa

Isso é diferente da exibição gráfica. Por exemplo, as opções do menu de dicas de ferramentas não se aplica à exibição de exploração. E, colocar o cursor sobre um símbolo não fará com que apareça a dica da ferramenta. Na exibição de exploração, as informações sobre o status são exibidas no painel à direita, na coluna **Estado**.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1466
Nº 3698
Doc

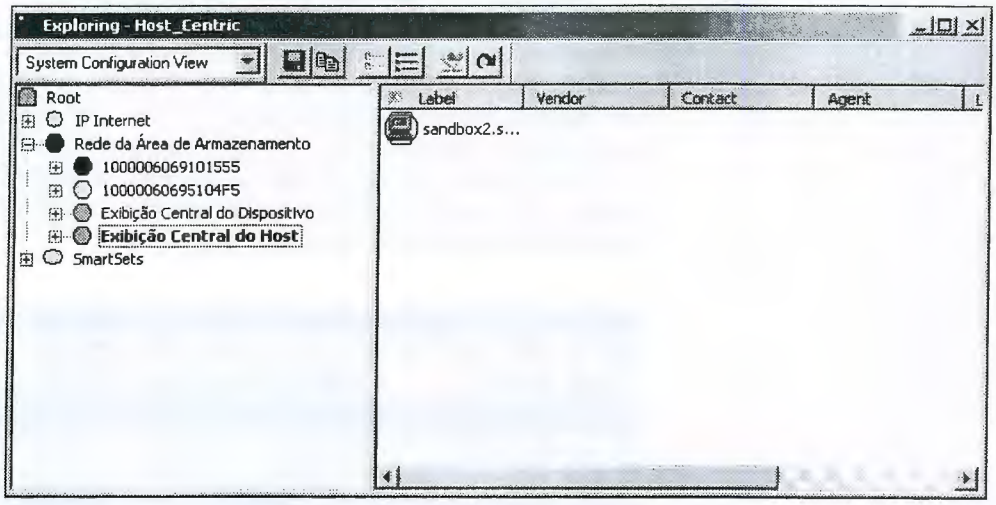


Figura 25. Opção de status da barra de ferramentas

Se sua opção de dicas de propriedade não estiver definida como **Status**, você poderá selecioná-la na lista drop-down de dicas de propriedade. Você pode selecionar essa exibição no menu drop-down, mostrado do lado esquerdo da Figura 25.

Limpando o Histórico de Status

O Tivoli Storage Area Network Manager mantém um histórico de discovery e utiliza esse histórico para determinar o status. Por exemplo, se um dispositivo descoberto anteriormente desaparecer do discovery atual, será atribuído a ele um status crítico. Se você não quiser mais que esse dispositivo seja relatado como crítico, deverá limpar o histórico de todos os dispositivos e reconstruir as exibições do submapa, da seguinte maneira:

1. Selecione **SAN → Configure Manager**, no menu do console. O diálogo Configuração da SAN é exibido.

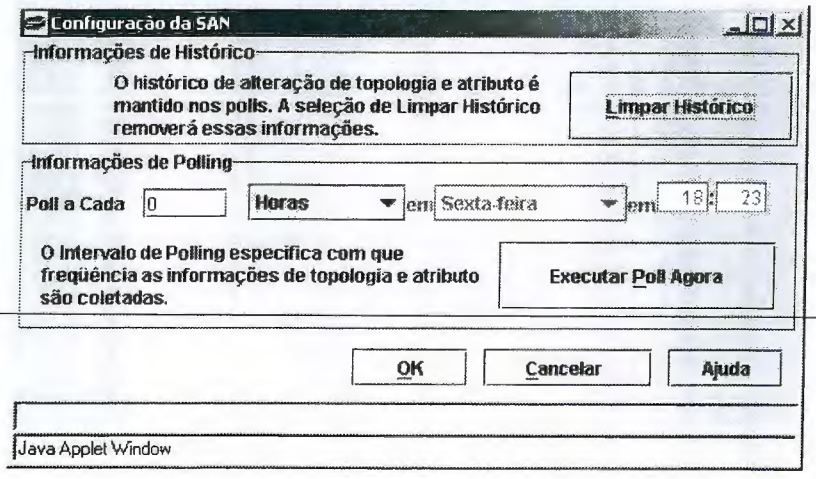


Figura 26. Limpando o histórico

2. Clique no botão **Limpar Histórico**.
3. Clique no botão **OK**.

Filtragem do Status

Se você tiver vários símbolos em sua tela, poderá filtrar alguns deles. Isso permite que você identifique rapidamente os dispositivos de um determinado status, como os dispositivos que não estejam no status normal. Para filtrar um determinado conjunto de símbolos, clique em um dos botões de cores, na barra de filtros de status, do lado direito da exibição. Clique nesse botão novamente para fazer com que os símbolos dessa cor reapareçam.

Figura 27. Filtrando um conjunto de símbolos

Descobrindo Dispositivos iSCSI

É possível iniciar a descoberta iSCSI através do menu do Tivoli NetView ou a partir da linha de comandos. Para executar a descoberta iSCSI, o Tivoli Storage Area Network Manager exige o seguinte:

- O Tivoli NetView precisa ter a descoberta IP ativada. O Tivoli NetView enviado com o Tivoli Storage Area Network Manager tem a descoberta IP desativada. Para obter detalhes sobre a configuração do ambiente para a descoberta de dispositivos iSCSI, consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide*.

  Nota: Quando a descoberta IP é ativada pode haver muita atividade na rede dependendo de quantos dispositivos estejam na rede. Quando o NetView é iniciado pela primeira vez, a região de gerenciamento IP padrão é o sistema no qual o programa NetView está operando e quaisquer redes IP às quais ele esteja conectado. O processo de descoberta gera o mapa da topologia Internet IP trabalhando para fora do sistema de gerenciamento.

  A descoberta IP pode ser controlada por um arquivo inicial que contém uma lista de endereços IP para o domínio de gerenciamento da SAN. É possível personalizar um arquivo inicial que descubra uma *parte* da rede IP conforme necessário. Consulte *Tivoli NetView for Windows User's Guide* para obter informações adicionais.

- Para gerenciar dispositivos iSCSI tais como iniciadores, destinos e chaves, é necessária uma definição de MIB iSCSI. Os dispositivos devem ser configurados de modo que o suporte a MIB iSCSI seja ativado e possam ser consultados por meio de SNMP. Por padrão, alguns dispositivos iSCSI têm seu suporte iSCSI desativado. Utilize o aplicativo de gerenciamento do dispositivo para ativar o suporte a iSCSI.

  É possível opcionalmente carregar arquivos de definição de MIB iSCSI se você desejar navegar os MIBs iSCSI. Consulte *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* para obter informações sobre o carregamento de arquivos de definição de MIB.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1467
Doc. 3698

- O dispositivo iSCSI deve primeiro ser descoberto como um dispositivo IP (conforme exibido no mapa da topologia Internet IP) antes que o Tivoli Storage Area Network Manager possa descobri-lo como um dispositivo iSCSI.

Quando se inicia uma descoberta iSCSI a partir do console do Tivoli NetView, um comando **nvsniffer** é ativado automaticamente o qual consulta todos os dispositivos IP descobertos quanto a suporte de iSCSI. Esse processo de descoberta identifica os dispositivos iSCSI a partir do mapa da topologia IP Internet e os inclui em um SmartSet iSCSI. O comando **nvsniffer** é um comando do NetView que toma sua entrada de um arquivo de configuração nvsniffer para consultar se os dispositivos são dispositivos iSCSI. Para obter informações adicionais, consulte o "nvsniffer" na página 76.

Você tem a opção de emitir manualmente o comando **nvsniffer** a partir de uma linha de comandos em vez de ativar a descoberta a partir do NetView. Consulte "nvsniffer" na página 76.

Nos dois casos, um dispositivo precisa primeiro ser um dispositivo IP descoberto e suas informações precisam estar armazenadas no banco de dados do NetView antes que o processo nvsniffer possa determinar se ele é um dispositivo iSCSI.

O suporte iSCSI do Tivoli Storage Area Network Manager pode ser utilizado independentemente ou em conjunto com a estrutura de gerenciamento iSNS (Internet Storage Naming Service). O protocolo iSNS é um protocolo para gerenciamento de dispositivos iSCSI. Os dispositivos de armazenamento e os hosts podem se auto-registrar com um servidor iSCSI. Subseqüentemente, os hosts podem consultar o servidor iSNS ou receber atualizações assíncronas do servidor iSNS quanto ao status de dispositivos de armazenamento. O protocolo iSNS permite que as funções do servidor iSNS sejam implementadas em uma variedade de dispositivos, tais como: chaves, roteadores, controladores de armazenamento e nós de console de gerenciamento. Se o iSNS for utilizado com o Tivoli Storage Area Network Manager, é possível carregar os arquivos de MIB iSNS e utilizar o navegador MIB do Tivoli NetView para consultar o servidor iSNS e exibir o status de dispositivos iSCSI. Para obter informações adicionais sobre iSCSI e iSNS, consulte o seguinte Web site:

`http://www.ietf.org`

Iniciando a Descoberta iSCSI

Para iniciar a descoberta iSCSI a partir do menu do console do Tivoli NetView selecione **Tools → iSCSI Operations**.

A Figura 28 na página 39 mostra que você tem as seguintes opções de descoberta iSCSI:

- All iSCSI Devices
- All iSCSI Initiators
- All iSCSI Targets

10355
A.

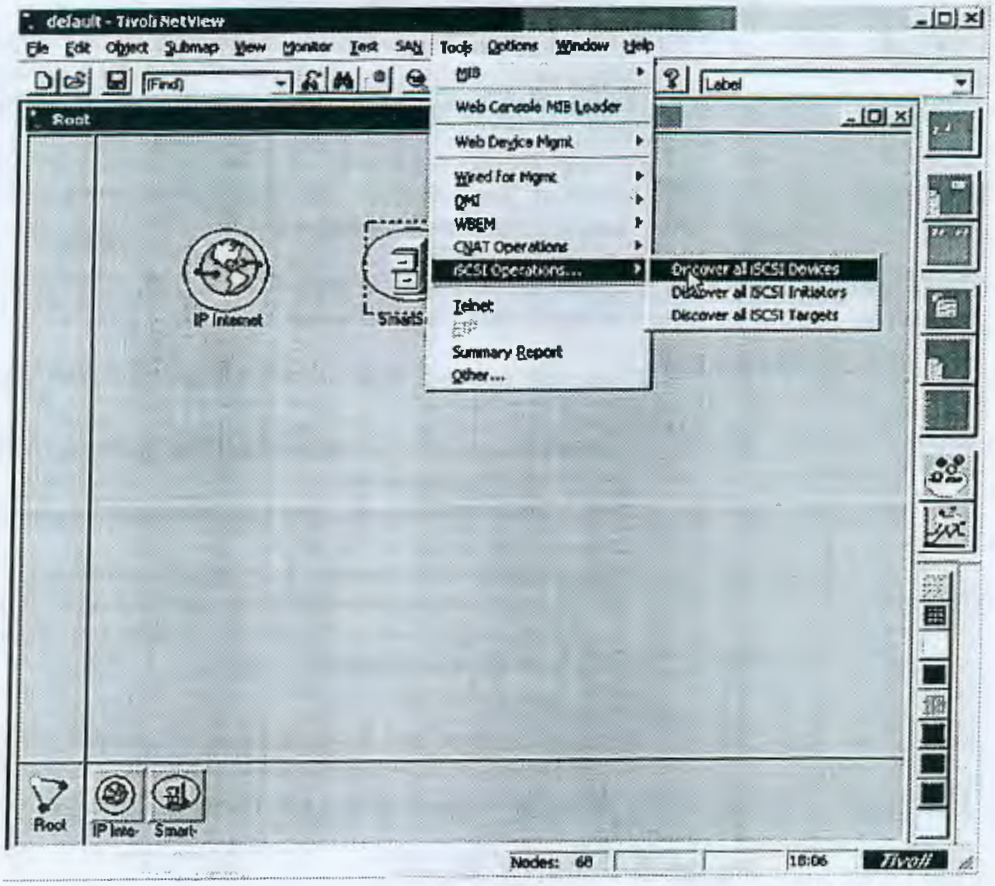


Figura 28. Iniciando a descoberta iSCSI

Somente é preciso iniciar a descoberta iSCSI uma vez. Se você selecionar esta opção uma segunda vez, terá várias descobertas em andamento. Esta ação pode produzir resultados inesperados.

O tempo de polling padrão é a cada 60 minutos. Se você desejar alterar o tempo de polling, utilize o comando **nvsniffer**. Consulte "Replanejando o Polling iSCSI" na página 40 e "nvsniffer" na página 76.

O processo de descoberta cria um SmartSet semelhante à Figura 29 (iSCSI6). Para navegar para o painel do SmartSet, dê um clique duplo no ícone da raiz no lado esquerdo do painel do Tivoli NetView e, em seguida, dê um clique duplo no ícone do SmartSet.

Figura 29. Exemplo de SmartSet iSCSI

Dê um clique duplo no SmartSet iSCSI para visualizar seus membros.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1468
3698
Doc.

Replanejando o Polling iSCSI

O tempo de polling padrão de descoberta iSCSI é a cada 60 minutos. Se você desejar alterar o tempo de polling, deve emitir o comando **nvsniffers** e especificar o arquivo de configuração do tipo de descoberta que deseja alterar.

O Tivoli Storage Area Network Manager fornece três arquivos de configuração separados (um para cada uma das opções do menu iSCSI) no diretório \usr\ov\prg_samples\iscsi, a saquir:

- nvsniffer.conf (para todos os dispositivos iSCSI)
- nvsnifferini.conf (para iniciadores iSCSI)
- nvsniffertar.conf (para destinos iSCSI)

O exemplo a seguir mostra como replanejar o polling para todos os dispositivos iSCSI:

1. É preciso parar o polling iSCSI. Obtenha o *job_ID* da instância da descoberta iSCSI que deseja alterar.
   a. Clique na barra de Tarefas e, em seguida, clique em **Gerenciador de Tarefas**
   b. Clique na guia Processos.
   c. Localize nvsniffer.exe. A coluna PID identifica o *job_ID*. Você pode dar um clique com o botão direito do mouse no *job_ID* e, em seguida, clique em **Finalizar Processo**. Como alternativa, você pode utilizar o comando do Windows **at** e emitir:

      ```
      at <job_ID> /d
      ```
2. Altere o planejamento de polling para a descoberta de todos os dispositivos iSCSI para 90 minutos emitindo o seguinte comando:

   ```
   nvsniffer -c \usr\ov\prg_samples\iscsi\nvsniffer.conf -r 90
   ```

Parar o Polling iSCSI

É possível parar o polling iSCSI utilizando o Gerenciador de Tarefas do Windows ou o comando **at**.

1. Obtenha o *job_ID* da instância da descoberta iSCSI que deseja parar.
   a. Clique na barra de Tarefas e, em seguida, clique em **Gerenciador de Tarefas**
   b. Clique na guia Processos.
   c. Localize nvsniffer.exe. A coluna PID identifica o *job_ID*. Você pode dar um clique com o botão direito do mouse no *job_ID* e, em seguida, clique em **Finalizar Processo**. Como alternativa, você pode utilizar o comando do Windows **at** e emitir:

      ```
      at <job_ID> /d
      ```

103
A

Capítulo 4. Trabalhando com Recursos

O Capítulo 3, "Exibindo a Rede", na página 15 explicou como navegar por meio da topologia SAN até um dispositivo de rede específico. Este capítulo descreve as seguintes tarefas:

- "Iniciando Aplicativos de Dispositivos de Rede"
- "Utilizando SNMP para Gerenciar Eventos" na página 43
- "Utilizando Detecção de Erros e Isolamento de Falhas" na página 44

Iniciando Aplicativos de Dispositivos de Rede

Alguns dispositivos de rede, como dispositivos de armazenamento e comutadores Fibre Channel, contêm aplicativos para ajudar no gerenciamento e na configuração desses dispositivos. Para iniciar um aplicativo de dispositivo a partir do menu do console, clique em seu símbolo no submapa e clique em **SAN → Launch Application**.

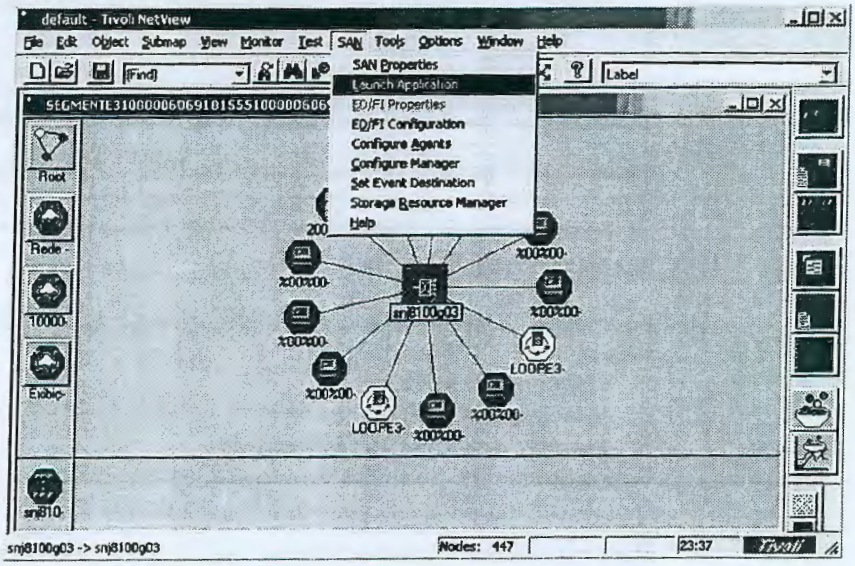


Figura 30. Iniciando um aplicativo

Se a opção **Launch Application** estiver desativada, o dispositivo não identificou um aplicativo de gerenciamento do Tivoli Storage Area Network Manager. Alguns dispositivos SAN têm aplicativos de gerenciamento, mas não suportam a arquitetura para identificar o nome do aplicativo. Você não pode iniciar esses aplicativos a partir do menu de contexto **Launch Applications**. Se tiver esse dispositivo, consulte "Uma Técnica Alternativa de Início" para obter um procedimento alternativo para iniciar.

Uma Técnica Alternativa de Início

Alguns dispositivos SAN têm aplicativos de gerenciamento, mas não suportam a arquitetura que identifica o nome do aplicativo. Você não pode iniciar esses aplicativos a partir do menu de contexto **Launch Applications**. Se tiver esse dispositivo, poderá ainda utilizar o Tivoli NetView para iniciar o aplicativo. Para

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1469
Doc. 3698

isso, clique com o botão direito do mouse no símbolo de um dispositivo no console do NetView e selecione **Object Properties**, no menu de contexto. O diálogo **Object Properties** é exibido (consulte a Figura 31).

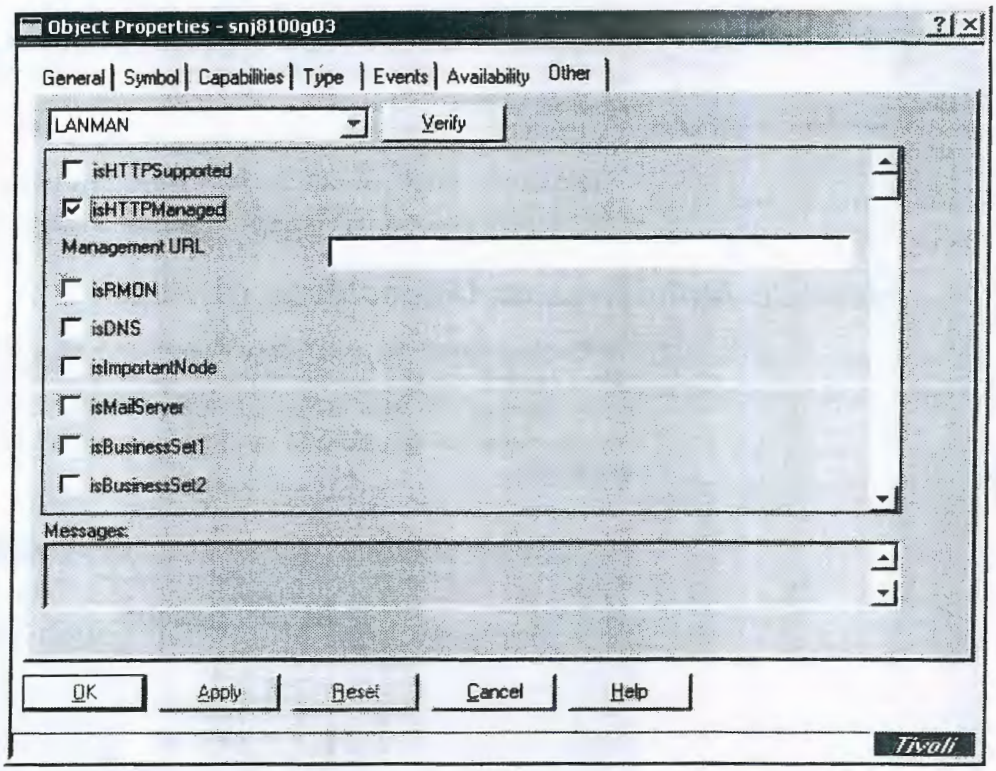


Figura 31. Object Properties

Execute as seguintes etapas para identificar o aplicativo de gerenciamento na Figura 31:

1. Clique na guia **Other**.
2. Selecione **LANMAN** nas opções, no canto superior esquerdo.
3. Marque a caixa **IsHTTPManaged**.
4. Digite o URL do aplicativo de dispositivo no campo **Management URL**.
5. Clique em **Verify** e, em seguida, em **Apply** e então em **OK**.

Para iniciar esse aplicativo, clique com o botão direito do mouse no símbolo do dispositivo e selecione **Management Page**, no menu de contexto (consulte a Figura 32 na página 43).

10350
A

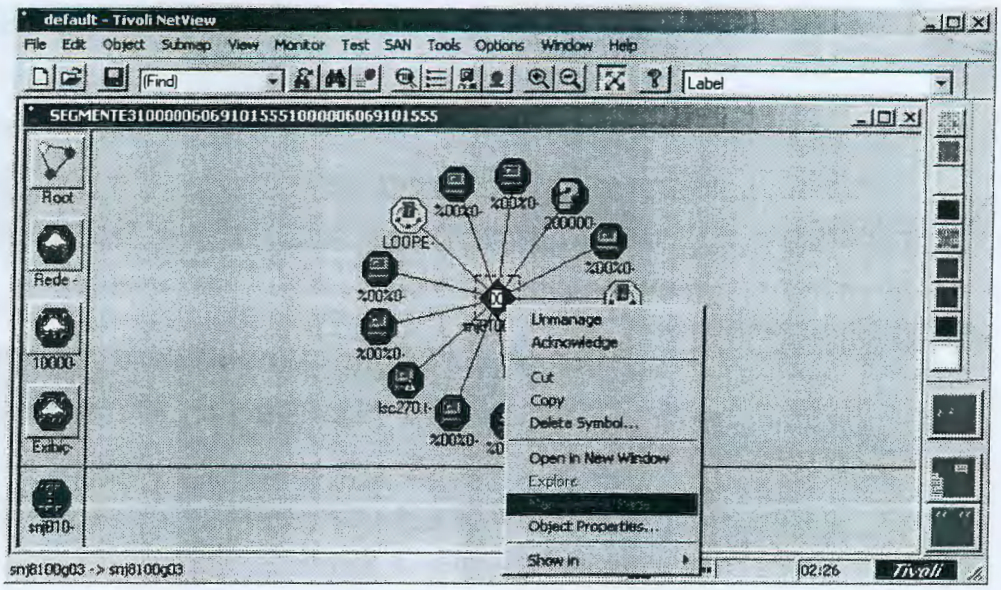


Figura 32. Iniciando pelo NetView

Utilizando SNMP para Gerenciar Eventos

Você pode utilizar o Tivoli NetView Event Browser para exibir eventos no banco de dados de eventos do Tivoli NetView. Como o Tivoli NetView pode gerenciar redes com base em IPs e SANs, o banco de dados de eventos pode conter eventos para ambos os tipos de redes.

- Consulte "Configurando o Destino de Eventos" na página 19 e o *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* para obter informações sobre como configurar o destino para traps do SNMP e eventos TEC.
- Consulte "Exibindo as Propriedades do Dispositivo da SAN" na página 29 para obter informações sobre como exibir informações do sensor a partir de um dispositivo e uma lista de eventos relatados pelo dispositivo.

Os seguintes tipos de eventos podem ser encontrados no banco de dados de eventos:

- Condições que o Tivoli NetView detecta, como um dispositivo em status crítico.
- Os traps do SNMP que são enviados a partir de dispositivos na rede IP, como de uma Ponte IP/Token Ring.
- Os traps do SNMP que são enviados a partir de dispositivos SAN, como de um comutador Fibre Channel.
- Os traps do SNMP que são enviados de produtos do Tivoli Storage Area Network Manager.

Para utilizar o Tivoli NetView Event Browser para exibir eventos no banco de dados de eventos do Tivoli NetView, execute as seguintes etapas:

1. Inicie o Tivoli NetView Event Browser, selecionando **Monitor → Events → All**, no menu do console. A janela Event Browser é exibida. Observe que essa exibição é alterada à medida que novos eventos ocorrem.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1407
Doc 3698

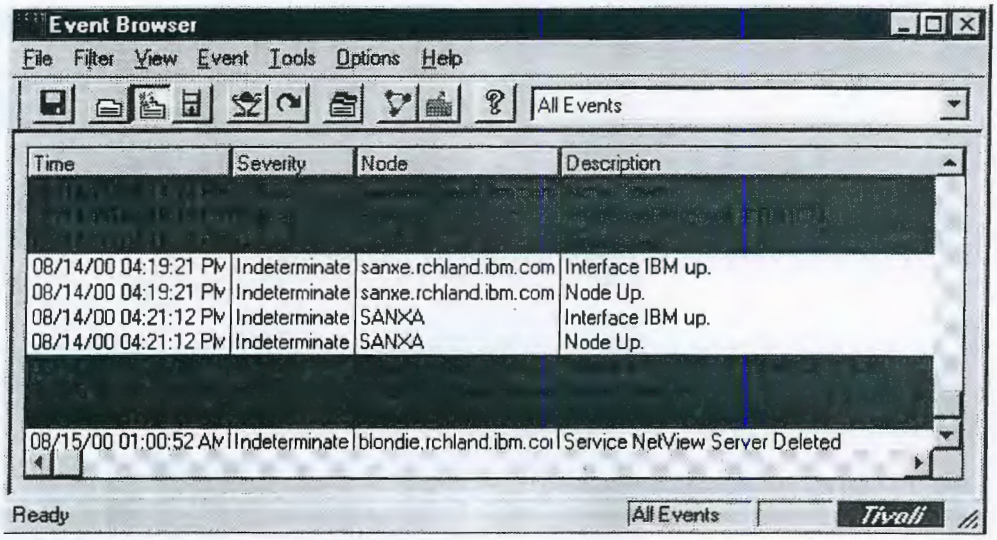


Figura 33. Navegador de Eventos

2. Clique com o botão direito do mouse em um evento para tornar visível um menu de contexto.
3. Clique em **Event Details** para exibir mais informações sobre um evento.

Utilizando Detecção de Erros e Isolamento de Falhas

O EDFI (Detecção de Erros e Isolamento de Falhas) ajuda na determinação de problemas em links de interconexão SAN Fibre Channel. O EDFI identifica o hardware com defeito pela utilização de análise de falhas previstas. O EDFI monitora dados de erros temporários através da SAN e os analisa quanto a padrões. O hardware muitas vezes falha de forma tal que condições intermitentes podem ser identificadas antes que se tornem uma falha permanente. O isolamento de falhas é executado para identificar o hardware com defeito.

O objetivo é identificar o dispositivo óptico e o hardware de interconexão com falha e notificar os usuários, que podem reparar ou substituir o hardware antes que a falha se torne permanente.

O EDFI não analisa erros para componentes internos tais como fontes de alimentação. Sua função é analisar contadores associados à transmissão de dados em links SAN.

- Uma taxa alta de erros temporários causa problemas de desempenho, os quais podem ser muito graves.
- Aguardar por uma falha permanente significa interrupção, reparo ou substituição de equipamentos não planejados.
- Algumas falhas (por exemplo, cabos rompidos) podem nunca ter um erro permanente mas podem deixar o sistema com um link degradado indefinidamente.
- Em resposta a erros intermitentes e repetitivos, os sistemas hosts, sistemas de armazenamento e procedimentos de recuperação de erro de componentes da SAN podem causar alterações imprevisíveis na configuração de E/S do sistema, da SAN Fibre Channel ou de ambas. Isso pode afetar a disponibilidade do sistema e do armazenamento.

10349
A

Quando o EDFI identifica um componente com falha, ele utiliza o Tivoli NetView para notificar o usuário. Depois que um erro tiver sido corrigido, você deve limpar imediatamente a indicação do erro.

Iniciando e Parando o EDFI

Para iniciar o EDFI, faça o seguinte:

1. Abra o ícone do Console Tivoli NetView no desktop. A partir do menu do Tivoli NetView, selecione **SAN → EDFI Configuration**.

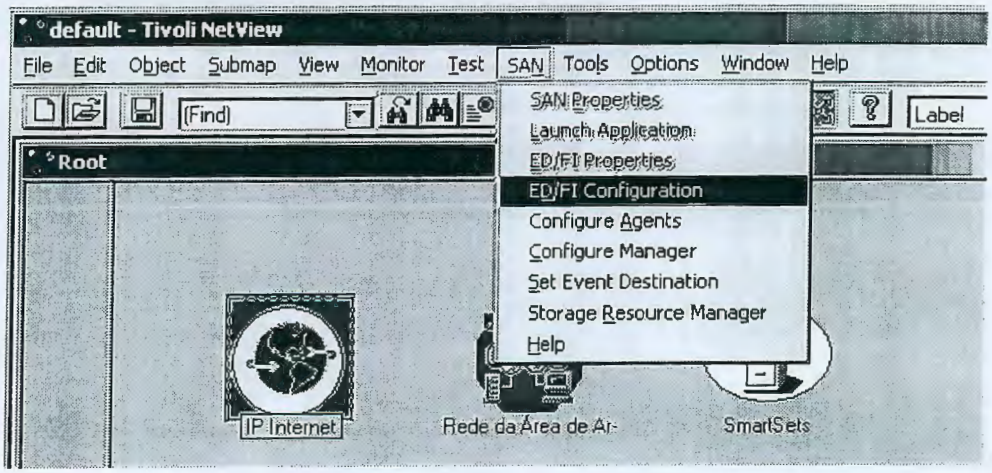


Figura 34. Iniciando ou Parando o EDFI

2. O painel Propriedades de Configuração de EDFI é exibido. Certifique-se de que o botão de opções Ativar Detecção de Erro e Isolamento de Falha esteja selecionado. Clique em **Ok** para consolidar a alteração e feche a janela ou clique em **Aplicar** para consolidar a alteração e deixar a janela aberta.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1471
Doc 3698

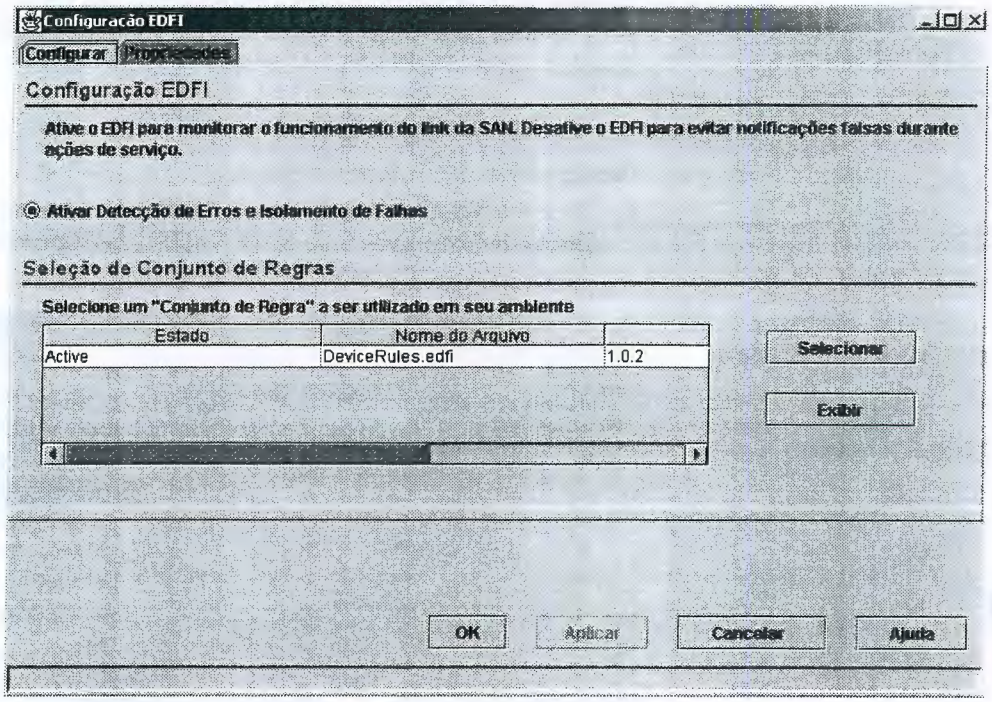


Figura 35. Painel Propriedades de Configuração de EDFI

Para parar o EDFI, faça o seguinte:

1. A partir do menu do Tivoli NetView, selecione **SAN → EDFI Configuration**.
2. No painel Propriedades de Configuração de EDFI, desmarque o botão de opções Ativar Detecção de Erro e Isolamento de Falha. Clique em **Ok** para consolidar a alteração e feche a janela ou clique em **Aplicar** para consolidar a alteração e deixar a janela aberta.

Nota: Para evitar que notificações de erro falsas apareçam na SAN, desative o EDFI durante a instalação e reconfiguração de hardware da SAN. Para obter mais informações, consulte o "Identificando o Hardware com Defeito" na página 53.

Relatório de Eventos EDFI

O EDFI gera eventos padrões do Tivoli Enterprise Console que podem ser utilizados para fins de relatório. Os tipos de eventos para o EDFI são:

Início de serviço EDFI
Este evento é emitido quando o EDFI tiver sido iniciado.

Parada de serviço EDFI
Este evento é emitido quando o EDFI tiver sido parado.

Notificação de dispositivo EDFI
Este evento é emitido quando o EDFI tiver uma notificação para relatar.

Limpeza de notificação de dispositivo EDFI
Este evento é emitido quando o evento tiver sido limpo.

A notificação EDFI é configurada utilizando os mecanismos padrões de relatório de eventos do Tivoli.

10347

Trabalhando com Conjuntos de Regras

Os conjuntos de regras contêm limites e critérios que são utilizados na análise de falhas previstas e no isolamento de falhas. Para que o EDFI utilize um conjunto de regras, ele deve ser carregado no Tivoli Storage Area Network Manager, selecionado e consolidado clicando em **Ok** ou em **Aplicar** no painel Configuração EDFI.

Carregando um Conjunto de Regras

Os produtos de hardware mudam freqüentemente. Você deve verificar os conjuntos de regras disponíveis com o Tivoli Storage Area Network Manager em relação aos conjuntos de regras recomendados disponíveis no site de suporte do IBM Tivoli Storage Area Network Manager. Se o site recomendar um conjunto de regras diferente, copie-o para o seguinte diretório na máquina do gerenciador:

```
$path\tivoli\itsanm\manager\conf\edfi
```

Em seguida, o conjunto de regras aparece automaticamente na lista de conjuntos de regras disponíveis para seleção (consulte Figura 35 na página 46). Se uma nova regra for copiada para o diretório correto mas não parecer na lista de regras disponíveis para seleção, ela pode ter sido identificada como corrompida pelas verificações de consistência do EDFI. Se for esse o caso, existirá uma entrada no arquivo msgITSANM.log.

Os conjuntos de regras são identificados pelos seguintes campos:

Estado

Ativo O conjunto de regras está sendo utilizado pelo EDFI. Somente um conjunto de regras pode estar ativo por vez.

Não Ativo
O conjunto de regras não está selecionado e não está sendo utilizado pelo EDFI.

Selecionado
O conjunto de regras foi selecionado. Somente um conjunto de regras pode ser selecionado por vez. Um conjunto de regras selecionado pode se tornar o conjunto de regras ativo, clicando no botão **Ok** ou **Aplicar**.

Arquivo
Nome do arquivo no sistema de arquivos local.

Versão
O número da versão do conjunto de regras. O número da versão é no formato de XX.YY.ZZ, onde:

XX O número de revisão principal

YY O número de revisão secundário.

ZZ O número de revisão incremental.

Descrição do Conjunto de Regras
Um nome curto que identifica o conjunto de regras. Ele descreve resumidamente as características únicas do conjunto de regras.

Exibindo e Selecionando um Conjunto de Regras

Para exibir e selecionar um conjunto de regras que tenha sido carregado, faça o seguinte:

1. Abra o ícone do Console Tivoli NetView no desktop. A partir do menu do Tivoli NetView, selecione: **SAN → EDFI Configuration**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1179
3698
Doc.

2. O painel Propriedades de Configuração de EDFI é exibido (consulte a Figura 35 na página 46). Clique em **Ok**.
3. Na janela Configuração de EDFI, selecione o painel Configurar, realce o conjunto de regras desejado e faça o seguinte:
   - Para exibir, clique em **Exibir**.
   - Para selecionar um arquivo de regras para ser utilizado como o conjunto de regras ativo, clique em **Selecionar**. Em seguida, clique em **Ok** ou **Aplicar** para consolidar a alteração.

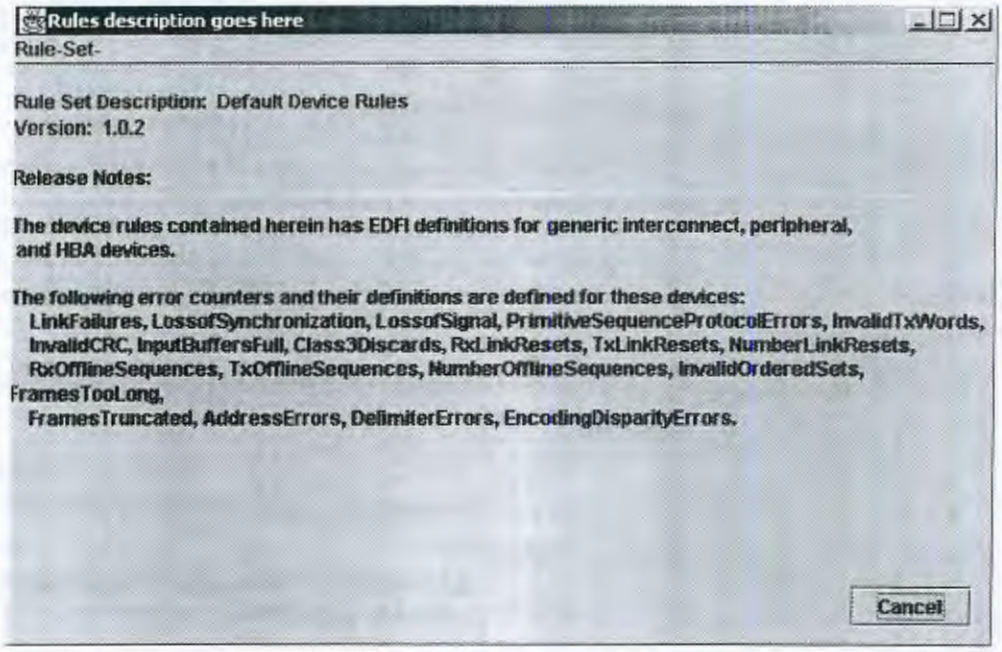


Figura 36. Painel Regras de EDFI

Gerenciando um Evento EDFI

Normalmente, quando um evento EDFI é relatado, ainda não ocorreu uma falha permanente. Para responder a um evento, faça o seguinte:

1. Vá para o console do gerenciador SAN e localize a notificação de erro EDFI.
2. Utilize a notificação de erro EDFI para localizar o link com falha.
3. Utilize diagnósticos específicos do dispositivo e guias de determinação de problemas para isolar o hardware com defeito no link.
4. Repare ou substitua o hardware identificado o mais breve possível.
5. Depois que o hardware identificado for reparado ou substituído, limpe a notificação de erro.

As etapas são descritas em detalhe nas seções a seguir.

Exibindo uma Notificação de Erro

Quando o EDFI identifica um hardware com defeito, ele coloca uma notificação do Log de Propriedades EDFI. Para exibir o log, faça o seguinte:

1. A partir do menu do Tivoli NetView, selecione **SAN → EDFI Configuration**. A janela Propriedades de Configuração EDFI aparece.
2. Clique na guia **Propriedades**:

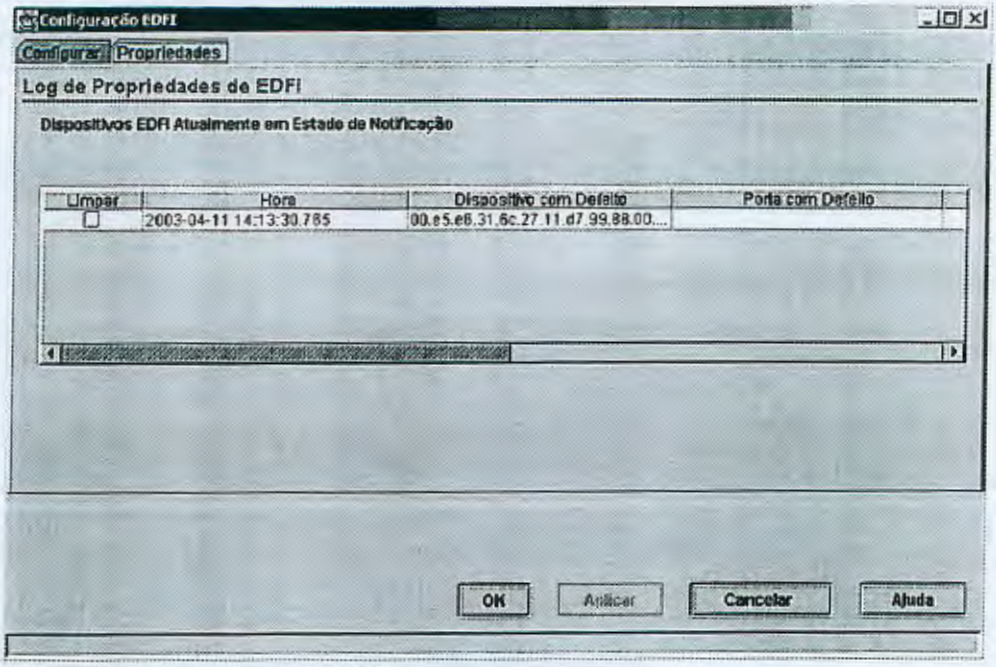


Figura 37. Log de Propriedades EDFI

O EDFI somente isola até o link. A notificação inclui os seguintes campos que podem ajudar a identificar o hardware:

Hora A hora em que o registro da notificação foi criado ou atualizado.

Dispositivo com Defeito
O nome de nó world wide Fibre Channel de um dispositivo no link.

Porta com Defeito
O nome de porta world wide Fibre Channel de uma porta no link.

Dispositivo Indicado
O nome de nó world wide Fibre Channel de um dispositivo relacionado onde o erro foi detectado primeiro.

Porta Indicada
O nome de porta world wide Fibre Channel de uma porta relacionada onde o erro foi detectado primeiro.

Contador
O contador de erros primário que foi utilizado na identificação da falha.

Regra Estatística
O identificador da regra no conjunto de regras utilizado na análise de falhas previstas para a notificação.

Versão da Regra
Um número que identifica a versão da regra utilizada na identificação da falha.

Referência de PD
Referência de determinação de problemas - um identificador exclusivo para um guia de determinação de problemas.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1473
Nº 3698
Doc.

Notificação Visual EDFI: Além de registros de notificação, o EDFI adiciona o símbolo de notificação ⚠ ao símbolo do dispositivo na exibição da topologia. Por exemplo:

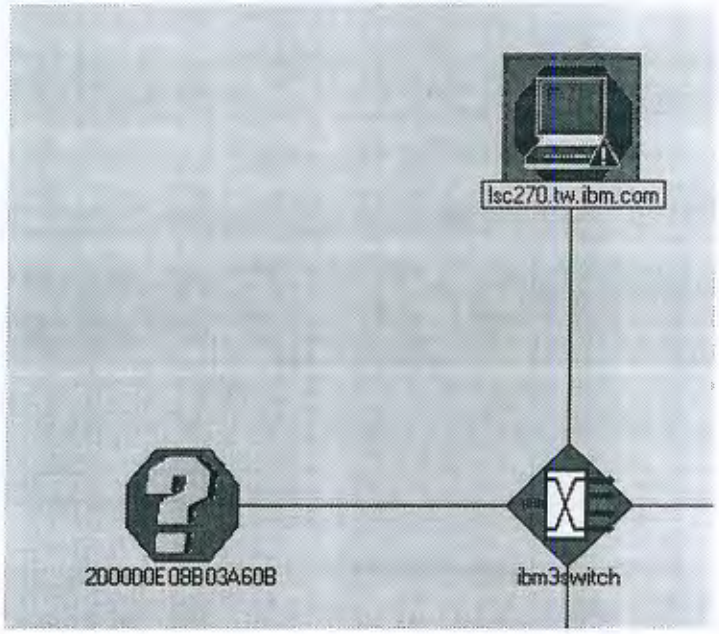


Figura 38. Símbolo de notificação em um ícone de dispositivo

Você pode encontrar informações mais detalhadas sobre um dispositivo que tem um símbolo de notificação, faça o seguinte:

1. A partir da exibição da topologia, selecione o dispositivo com o símbolo (consulte a Figura 38).
2. No menu de opções da SAN, selecione Propriedades EDFI. A janela Propriedades - EDFI é exibida.

A Configuração EDFI contém os registros de notificação para toda a SAN; as Propriedades EDFI contêm o registro de notificação somente para o dispositivo selecionado. Se o dispositivo não for selecionado, o menu Propriedades EDFI não poderá ser selecionado e estará esmaecido.

Localizando um Erro na Topologia da SAN

Não é aparente em um registro de notificação onde ocorreu um erro na topologia. Contudo, o registro da notificação fornece um nome world wide que pode ser utilizado para pesquisas. Se a SAN for pequena, ele pode ser encontrado simplesmente procurando o símbolo de notificação (⚠) na exibição da topologia.

Para SANs maiores, você pode utilizar o nome world wide do dispositivo como um ID de objeto na função Localizar sob o menu de opções Editar. Consulte Figura 39 na página 51. O nome world wide do dispositivo é também o ID do objeto utilizado pelo Tivoli NetView.

10343
A.

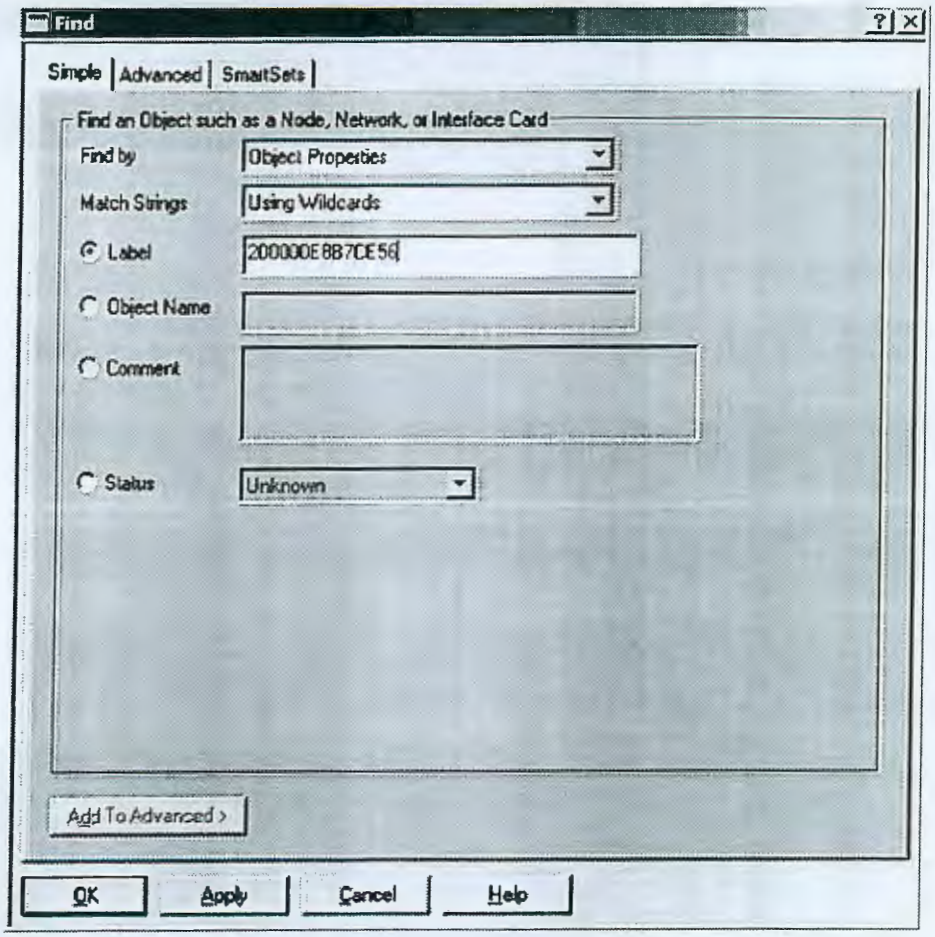


Figura 39. Função Localizar no menu de opções Editar

Outra maneira de localizar um dispositivo que tenha uma notificação EDFI é esta:

1. Na janela Find, selecione a guia Advanced. Consulte Figura 40 na página 52.
2. No campo Combine Find Conditions, especifique `("isEDFI"="True")` e clique em **Ok** ou **Apply**. Uma lista das localizações dos itens é exibida na janela Found Objects.
3. Selecione um item nessa lista para exibir esse item na topologia. Consulte Figura 41 na página 53.

RQS nº 03/2005 - CN
Fls 1 3698
Doc.

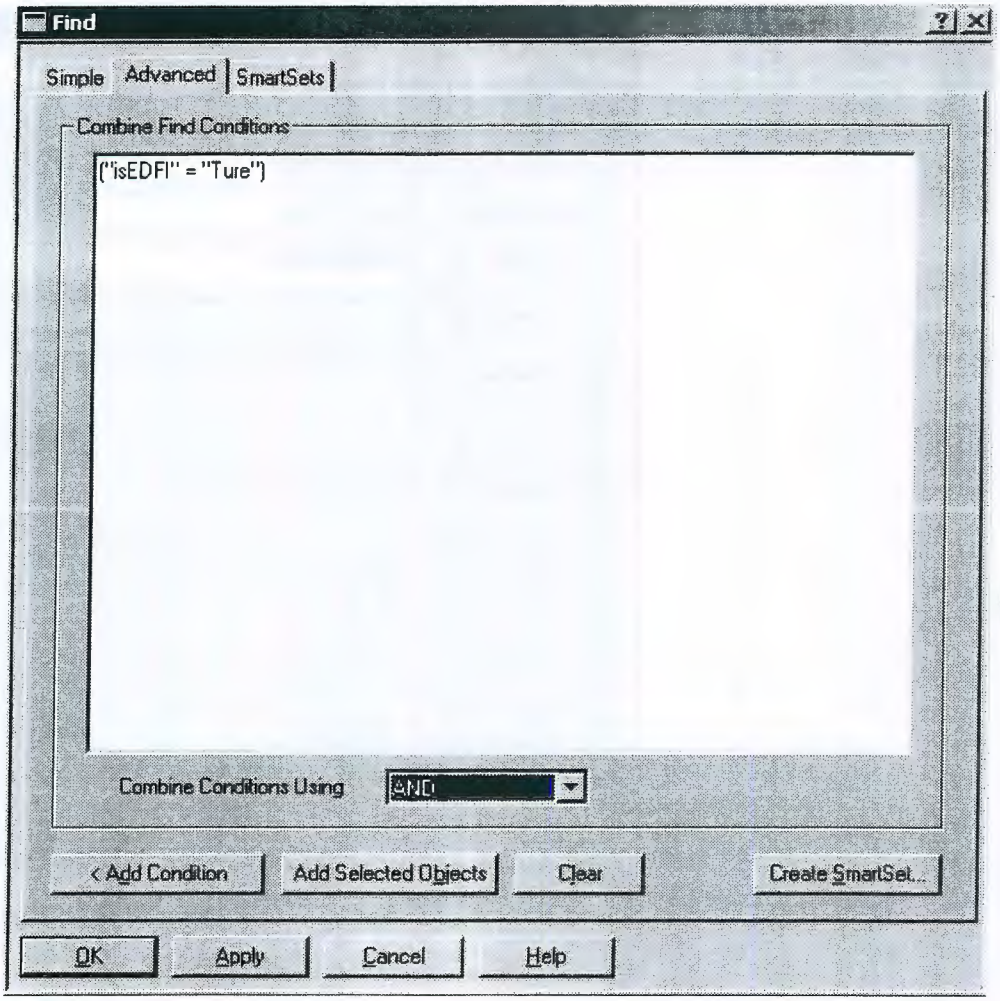


Figura 40. Janela Find

10341
A.

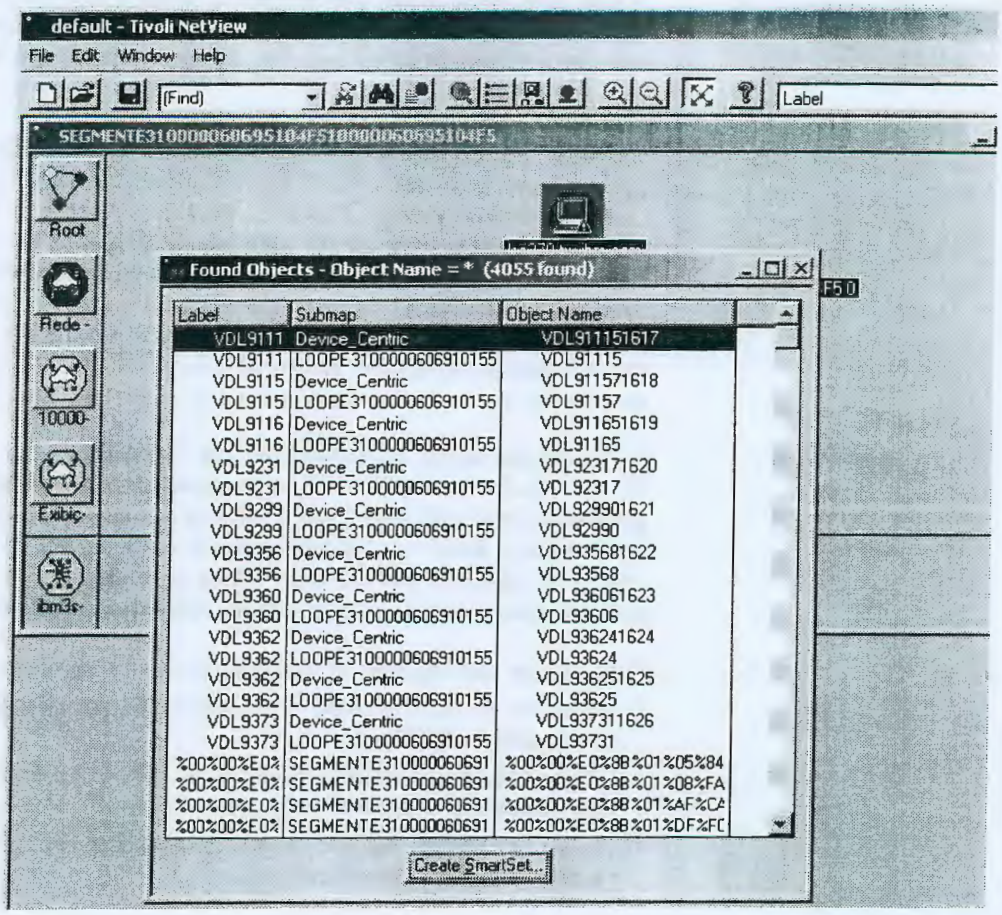


Figura 41.

Identificando o Hardware com Defeito

O registro da notificação fornece informações detalhadas que podem ser utilizadas para identificar o hardware com defeito. Os dois campos principais a examinar são Dispositivo com Defeito e Porta com Defeito. Esses campos apontam para o dispositivo e a porta no lado da transmissão da falha, o qual é o lado com mais probabilidades de estar com falha. Alguns problemas possíveis são:

- Módulo SFP ou GBIC com falha em qualquer lado do link
- Cabos rompidos ou conectores empoeirados
- Comprimento excessivo do cabo
- Número excessivo de acopladores de cabo intermediários

O EDFI pode isolar falhas somente até o nível do link. Portanto, qualquer lado do link ou o próprio cabo pode ser o componente com falha. Antes de substituir o hardware, consulte seus contratos de serviço e guias de determinação de problemas do produto para orientação. A limpeza, o encaixe dos cabos e a execução de diagnósticos são algumas das etapas que podem ser recomendadas para chegar a uma decisão definitiva sobre o reparo ou substituição de peças.

Se você puder identificar um componente, deve diagnosticar o problema e reparar ou substituir o componente assim que possível antes que ocorra uma falha permanente. Se não puder identificar um componente, no mínimo deve monitorar

RQS nº 03/2005 CN
Fls. Nº 1475
3698
Doc.

o link para obter erros. Em ambientes onde a disponibilidade alta dos sistemas é uma exigência ou existirem contratos de nível de serviço no local, você deve entrar em contato com os representantes de serviço sobre a substituição de componente de Fibre Channel.

Ações de serviço, como um ciclo de energia e a substituição de peças, às vezes podem fazer com que o EDFI envie notificações falsas para os dispositivos que estão recebendo serviço. Portanto, você deve desativar o EDFI durante essas instalações. Esses eventos em geral são bloqueados pelas funções de análise do EDFI, mas a desativação do EDFI evita qualquer possibilidade de confusão. Se uma notificação EDFI aparecer dentro de algumas horas em seguida a uma instalação ou reconfiguração de hardware onde o EDFI não estiver desativado (especialmente ações que levem uma hora ou mais), pode ser interessante limpar a notificação e ver se ela reaparece antes de efetuar uma ação de reparo.

Limpando uma Notificação de Erro

O símbolo de notificação EDFI não desaparece automaticamente depois que o problema tiver sido corrigido. Como as contagens de erros temporários são analisadas, o EDFI não pode distinguir a nova peça da antiga (diferentemente do que seria esperado em casos de falhas permanentes na SAN). É importante limpar a notificação quando o hardware for substituído para evitar confusão.

Para limpar um registro de notificação, faça o seguinte:

- No menu de opções SAN, selecione o submenu Propriedades EDFI ou Configuração EDFI.
- Clique em um ou mais quadrados na coluna Limpar do Log de Propriedades EDFI (consulte Figura 37 na página 49).
- Clique em **Ok** ou **Aplicar**. Sair da janela sem clicar em **Ok** ou **Aplicar** cancela o pedido para limpar as notificações.

10339
A

Parte 2. Apêndices

© Copyright IBM Corp. 2002, 2003

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1476
Nº 3698
Doc.

10338
A.

Apêndice A. Referência de Comandos

Os comandos do IBM Tivoli Storage Area Network Manager permitem que você execute operações no sistema a partir de uma interface da linha de comando. Isso é útil quando você não tem acesso a uma exibição gráfica, como ao executar comandos sobre uma conexão dial-up ou criar scripts que submetam comandos.

Os comandos do IBM Tivoli Storage Area Network Manager são divididos em dois grupos:

- Comandos de Serviço de Registro – permitem que você configure e ative ou desative o registro de mensagens.
- Comandos de Service Manager – permitem que você exiba ou defina valores no arquivo de propriedades do usuário.

Os comandos deste capítulo são apresentados em ordem alfabética e contêm as seguintes informações:

- Uma descrição do comando.
- Um diagrama de sintaxe do comando. Consulte "Lendo Diagramas de Sintaxe" para obter uma explicação sobre esses diagramas.
- Descrições detalhadas dos parâmetros de comandos. Se o parâmetro for uma constante (um valor que não se altera), a abreviatura mínima aparecerá em letras maiúsculas.
- Exemplos do uso do comando.

Lendo Diagramas de Sintaxe

Esta seção descreve como ler os diagramas de sintaxe utilizados neste manual. Para ler um diagrama de sintaxe, siga o caminho da linha. Leia da esquerda para a direita, e de cima para baixo.

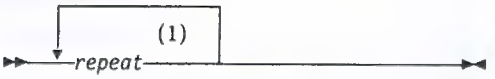
- O símbolo ▸▸— indica o início de um diagrama de sintaxe.
- O símbolo —▸ no final de uma linha indica que o diagrama de sintaxe continua na próxima linha.
- O símbolo ▸— no início de uma linha indica que o diagrama de sintaxe é continuação da linha anterior.
- O símbolo —▸◂ indica o fim de um diagrama de sintaxe.

Os itens da sintaxe, como uma palavra-chave ou uma variável, podem estar:

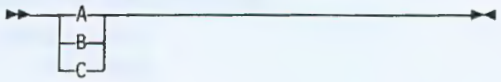
- Na linha (elemento obrigatório)
- Acima da linha (elemento padrão)
- Abaixo da linha (elemento opcional).

© Copyright IBM Corp 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1477
Doc: 3698

Descrição do Diagrama de Sintaxe	Exemplo
Abreviaturas: Letras maiúsculas indicam o menor truncamento aceitável. Se um item aparecer inteiramente em letras maiúsculas, ele não poderá ser truncado. Você pode digitar o item em qualquer combinação de letras maiúsculas ou minúsculas. Neste exemplo, você pode inserir KEYWO, KEYWORD ou KEYWOrd.	
Símbolos: Insira estes símbolos exatamente como eles aparecem no diagrama de sintaxe.	* Asterisco { } Chaves : Dois pontos , Vírgula = Sinal de Igual - Hífen () Parênteses . Ponto Espaço
Variáveis: Itens em letras minúsculas e em itálico (*var_name*) indicam variáveis. Neste exemplo, você pode especificar um *var_name* ao inserir o comando KEYWORD.	
Repetição: Uma seta virada para a esquerda significa que você pode repetir o item. Um caractere ou espaço dentro da seta significa que você deve separar os itens repetidos com esse caractere ou espaço. Uma nota de rodapé ao lado da seta indica o número de vezes que você pode repetir o item.	  **Notas:** 1 Especifique *repeat* até 5 vezes.

10336
A.

Descrição do Diagrama de Sintaxe	Exemplo
Opções obrigatórias: Quando dois ou mais itens estiverem em empilhados e um deles estiver na linha, você *deverá* especificar o item. Neste exemplo, você *deve* escolher A, B ou C.	
Escolha opcional: Quando um item estiver abaixo da linha, esse item será opcional. No primeiro exemplo, você pode escolher A ou nenhum. Quando dois ou mais itens estiverem empilhados abaixo da linha, todos eles são opcionais. No segundo exemplo, você pode escolher A, B, C ou nenhum deles.	
Padrões: Os padrões ficam acima da linha. O padrão é selecionado, a menos que você o substitua. Você pode substituir o padrão, incluindo uma opção da pilha abaixo da linha. Neste exemplo, A é o padrão. Você pode substituir A, escolhendo B ou C. Também é possível especificar o padrão explicitamente.	
Escolhas repetidas: Uma pilha de itens seguida por uma seta virada para a esquerda significa que você pode selecionar mais de um item ou, em alguns casos, repetir um único item. Neste exemplo, você pode escolher qualquer combinação de A, B ou C.	
Fragmentos de sintaxe: Alguns diagramas, devido ao comprimento, devem fragmentar a sintaxe. O nome do fragmento aparece entre barras verticais no diagrama. O fragmento expandido aparece entre barras verticais no diagrafna, após um cabeçalho com o mesmo nome do fragmento.	 **O nome do fragmento:**

RQS nº 03/2005 - CN
Fls. Nº 1478
Doc 3698

Inserindo Comandos

Um comando pode incluir o nome do comando e os parâmetros associados (se aplicável):

Nome do comando

A primeira parte de um comando é o nome do comando. O nome do comando consiste em um objeto, como *log*, e a ação a ser executada nesse objeto. Por exemplo, o comando a seguir define as propriedades para o arquivo de log de mensagens:

```
log set
```

Parâmetros

Os comandos podem ter parâmetros obrigatórios, opcionais ou não ter parâmetros. Siga estas regras gerais ao inserir parâmetros de comandos:

- Ao inserir parâmetros com um comando, sempre o anteceda com um traço (–).
- Digite mais de um parâmetro em qualquer ordem, após o comando. Separe os parâmetros com um espaço em branco.

Para emitir um comando no Windows, siga estas etapas:

1. Abra uma janela do prompt de comandos.
2. Vá para o diretório: *<diretório de instalação>\manager\bin\w32–ix86*. O diretório de instalação padrão é tivoli\itsanm\manager\bin\w32–ix86
3. Insira o seguinte comando: **setenv**.
4. Insira o comando. Por exemplo:

```
srmcp -u <user_ID> -p <password> [command]
```

Para emitir um comando no AIX, siga estas etapas:

1. Abra uma janela do terminal.
2. Altere o diretório para: *<diretório de instalação>/agent/bin/aix*. O diretório de instalação padrão é /tivoli/itsanm/agent/bin/aix
3. Insira o seguinte comando: **. ./setenv.sh**. Quando inserir . ./, observe que existe um espaço entre os pontos.
4. Insira o comando. Por exemplo:

```
./srmcp.sh -u <user_ID> -p <password> [command]
```

Para emitir um comando no Linux, siga estas etapas:

1. Abra uma janela do terminal.
2. Altere o diretório para: *<diretório de instalação>/agent/bin/linux* . O diretório de instalação padrão é /tivoli/itsanm/agent/bin/linux
3. Insira o seguinte comando: **. ./setenv.sh**. Quando inserir . ./, observe que existe um espaço entre os pontos.
4. Insira o comando. Por exemplo:

```
./srmcp.sh -u <user_ID> -p <password> [command]
```

Para emitir um comando no Solaris, siga estas etapas:

1. Abra uma janela do terminal.
2. Vá para o diretório: *<diretório de instalação>/agent/bin/solaris2*. O diretório de instalação padrão é /tivoli/itsanm/agent/bin/solaris2

3. Insira o seguinte comando: **. ./setenv.sh**. Quando inserir . ./, observe que existe um espaço entre os pontos.
4. Insira o comando. Por exemplo:

```
./srmcp.sh -u <user_ID> -p <password> [command]
```

Se você estiver inserindo comandos do IBM Tivoli Storage Area Network Manager a partir do host gerenciado ou de um console remoto, informe o URL do gerenciador. Por exemplo:

Windows

```
srmcp -url user1.mycity.ibm.com:9550 -u <ID_usuário> -p <senha>
[comando]
```

AIX, Linux e Solaris

```
./srmcp.sh -url user1.mycity.ibm.com:9550 -u <ID_usuário> -p <senha>
[comando]
```

Comandos de Serviço de Registro

Você pode configurar o IBM Tivoli Storage Area Network Manager para registrar ou gravar mensagens de texto de eventos do sistema, de modo que possa revisar essas ações posteriormente. Os comandos de registro de mensagens lhe ajudam a configurar o sistema para que reúna e envie essas informações aos arquivos de log de mensagens. É possível configurar o número, o tamanho, o tipo e o formato de seus arquivos de log de mensagens. Os seguintes tipos de mensagens são ativados por padrão:

Mensagens informativas
Indicam condições que são dignas de nota, mas que não requerem nenhuma precaução ou execução de uma ação.

Mensagens de aviso
Indicam condições que não requerem, necessariamente, uma ação do usuário. Por exemplo, uma parte de um programa não foi executada como planejado, mas os padrões foram aplicados, permitindo que o programa continue. Você deve examinar a saída para ver se é válida.

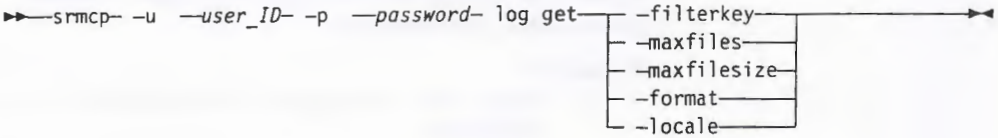
Mensagens de erro
Informam um usuário sobre eventos importantes, como falha de um componente ao gravar uma entrada do banco de dados.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1479
Doc: 3698

srmcp log get

O comando **srmcp log get** exibe as propriedades atuais do arquivo de log de mensagens. Se você não especificar um parâmetro para esse comando, será exibida uma mensagem de erro de sintaxe.

Sintaxe



Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

-filterkey
Exibe os tipos atuais de mensagens que são registradas no arquivo de log de mensagens.

-maxfiles
Exibe o número máximo atual de arquivos de log a serem criados.

-maxfilesize
Exibe o tamanho máximo atual do arquivo (em kilobytes) do log antes que um novo arquivo de log seja criado.

-format
Exibe o formato atual no qual as mensagens são salvas no arquivo de log de mensagens. As mensagens podem ser salvas no texto corrido ou formato XML.

-locale
Exibe a definição atual do locale de idioma no qual as mensagens são exibidas no arquivo de log de mensagens.

Exemplos

Tarefa Exibir os tipos atuais de mensagens que são registradas no arquivo de log de mensagens.

Comando: `srmcp -u user1 -p password1 log get -filterkey`

Tarefa Exibir o número máximo atual de arquivos de log a serem criados.

Comando: `srmcp -u user2 -p password2 log get -maxfiles`

Tarefa Exibir o tamanho máximo atual do arquivo (em kilobytes) do log, antes que um novo arquivo de log seja criado.

Comando: `srmcp -u user3 -p password3 log get -maxfilesize`

Tarefa Exibir o formato atual do log de mensagens.

Comando: `srmcp -u user4 -p password4 log get -format`

Tarefa Exibir a definição atual do locale de idioma no qual as mensagens são exibidas no arquivo do log de mensagens.

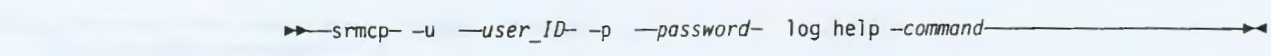
Comando: `srmcp -u user5 -p password5 log get -locale`

srmcp log help

10332
A.

O comando **srmcp log help** fornece informações gerais sobre os comandos de Serviço de Registro. O comando **srmcp log help** fornece informações sobre o comando específico com seus parâmetros.

Sintaxe



Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

-command
Você pode especificar estes comandos:
- get
- set

Exemplos

Tarefa Exibir informações sobre os comandos de Serviço de Registro.

Comando: `srmcp -u user1 -p password1 log help`

Tarefa Exibir informações sobre todos os parâmetros válidos do comando **srmcp log get**.

Comando: `srmcp -u user1 -p password1 log help -get`

Tarefa Exibir informações sobre todos os parâmetros válidos do comando **srmcp log set**.

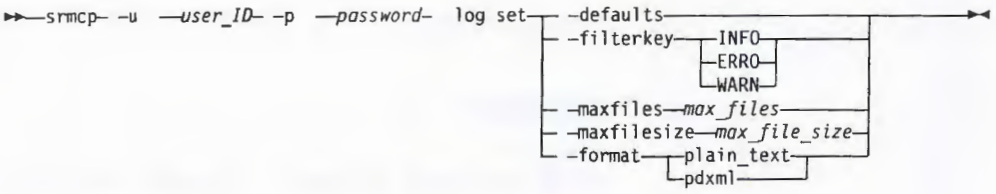
Comando: `srmcp -u user2 -p password2 log help -set`

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1480
3698
Doc

srmcp log set

O comando **srmcp log set** define as propriedades do arquivo de log de mensagens. Se você não especificar um parâmetro para esse comando, será exibida uma mensagem de erro de sintaxe.

Sintaxe



Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

-defaults
Redefine todas as definições de registro para as definições padrão.

-filterkey {INFO | ERROR | WARN}
Especifica os tipos de mensagens que serão registradas no arquivo de log de mensagens. Esses valores são sensíveis a maiúsculas e minúsculas. Os tipos são os seguintes:

INFO	Exibe mensagens de informação, aviso e erro.
ERROR	Exibe mensagens de erro.
WARN	Exibe mensagens de aviso e erro.

-maxfiles ***max_files***
Define o número máximo de arquivos de log a serem criados. Você deve especificar mais de um arquivo de log para ser criado, se desejar salvar entradas do log mais antigas. Se você especificar apenas um arquivo de log e ele ficar cheio, as entradas do log serão excluídas do arquivo de log e novas entradas serão incluídas.

-maxfilesize ***max_file_size***
Define o tamanho máximo do arquivo (em kilobytes) do log, antes que um novo arquivo de log seja criado.

-format {plain_text | pdxml}
Os valores são os seguintes:

plain_text	As mensagens são salvas no formato de texto corrido.
pdxml	As mensagens são salvas no formato XML.

Exemplos

Tarefa Redefinir os flags de mensagens flags para as definições padrão.

Comando: `srmcp -u user1 -p password1 log set -defaults`

Tarefa Exibir mensagens informativas, de erro e de aviso no arquivo de log.

Comando: `srmcp -u user2 -p password2 log set -filterkey INFO`

Tarefa Definir o número máximo de arquivos de log a serem criados até 10.

Comando: `srmcp -u user3 -p password3 log set -maxfiles 10`

Tarefa Definir o tamanho máximo do arquivo do log até 2.000 bytes, antes que um novo log seja criado.

Comando: `srmcp -u user4 -p password4 log set -maxfilesize 2000`

Tarefa Formatar o arquivo do log de mensagens no formato XML.

Comando: `srmcp -u user5 -p password5 log set -format pdxml`

10330
A-

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1481
Doc. 3698

A Comandos de Service Manager

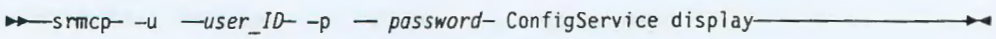
Os comandos de Service Manager permitem que você exiba ou defina os valores do arquivo de propriedades do usuário (tivoli/itsanm/manager/conf/user.properties), na máquina do gerenciador. Esse arquivo contém definições que controlam o registro do host, o destino dos traps do SNMP e o intervalo de monitoração do agente fora da banda. Os comandos de Service Manager a seguir são descritos em ordem alfabética.

10328
A.

srmcp ConfigService display

O comando **srmcp ConfigService display** exibe os valores no arquivo de propriedades do usuário (user.properties). Esse comando pode ser emitido somente no computador do gerenciador.

Sintaxe



Parâmetros

–u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

–p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

Exemplos

Tarefa Exibir os valores no arquivo user.properties.

Comando: `srmcp -u user1 -p password1 ConfigService display`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1482
Nº Doc. 3698

srmcp ConfigService get

O comando **srmcp ConfigService get** exibe o valor do nome de propriedade no arquivo de propriedades do usuário (user.properties) que você especifica. Esse comando pode ser executado somente no computador do gerenciador.

Sintaxe

```
►►—srmcp— -u —user_ID— -p —password— ConfigService get property_name————►◄
```

Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

property_name
Especifica o nome de propriedade no qual você deseja exibir o valor atual.

Exemplos

Tarefa Exibir o valor da propriedade **SnmpCommunityName** no arquivo user.properties.

Comando:
```
srmcp -u user2 -p password2 ConfigService get SnmpCommunityName
```

Tarefa Exibir o valor para uma propriedade de descoberta completa (**FullAttributeScan**) no arquivo user.properties.

Comando:
```
srmcp -u user2 -p password2 ConfigService get FullAttributeScan
```

Tarefa Exibir o URL para a propriedade (**SRMURL**) do Tivoli Storage Resource Manager no arquivo user.properties.

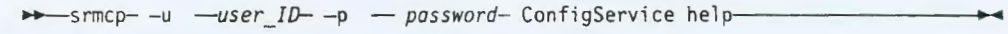
Comando:
```
srmcp -u user2 -p password2 ConfigService get SRMURL
```

10326
LA.

srmcp ConfigService help

O comando **srmcp ConfigService help** fornece ajuda sobre como utilizar os comandos do Manager Service.

Sintaxe



Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

Exemplos

Tarefa Exibir ajuda para os comandos **srmcp ConfigService**.

Comando: `srmcp -u user1 -p password1 ConfigService help`

RQS nº 03/2005 - CN
Fls. Nº 1483
Doc. 3698

10325
A.

srmcp ConfigService set

O comando **srmcp ConfigService set** define o valor da propriedade especificada para um novo valor no arquivo de propriedades do usuário (user.properties). Esse comando pode ser executado somente no computador do gerenciador.

Sintaxe

```
►►—srmcp— -u —user_ID— -p —password— ConfigService set property_name value————►◄
```

Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

property_name
Define o valor da propriedade especificada. *Property_name* pode ser:

FullAttributeScan *value*
Define o valor para uma descoberta completa. Os valores padrões para uma descoberta completa são definidos da seguinte maneira:

- IBM Tivoli Storage Area Network Manager para SAN Management - executar uma descoberta completa quando o usuário selecionar Poll Now e quando uma descoberta periódica ou planejada for iniciada.
- IBM Tivoli Storage Area Network Manager Bonus Pack para SAN Management - nunca executar uma descoberta completa.

Value pode ser:

Never Nunca executar uma descoberta completa (somente descoberta de topologia). Somente informações de nível superior são apresentadas nas exibições centrais no dispositivo e no host. Quando você altera esse valor de Never para outra definição do atributo, os dados que estiverem atualmente no banco de dados são exibidos nas exibições centrais no dispositivo e no host. Nesse ponto, os dados no banco de dados podem ser dados antigos e podem não representar a exibição lógica real. As informações do banco de dados são atualizadas depois que a próxima descoberta completa for executada.

PollNow
Somente executar uma descoberta completa quando o usuário selecionar **Poll Now**.

TimeBased
Somente executar uma descoberta completa quando uma descoberta periódica ou planejada for iniciada.

PollNowAndTimeBased
Executar uma descoberta completa quando o usuário selecionar **Poll Now** ou quando uma descoberta periódica ou planejada for iniciada.

hostPollingInterval
Define o intervalo de polling (em milissegundos) no qual ocorre o polling do host. O padrão é 60.000 (60 segundos).

OutbandAgentMonitorInterval *value*
Define o intervalo de monitoração (em milissegundos) do agente fora da banda.

SRMURL
Define o nome completo do host do gerenciador (não o host local). O padrão é:
`http://<host>:9530/ITSRM/TivoliSRM.html`

SnmpCommunityName
Define o nome da comunidade do SNMP.

SnmpTrapPort
Define o número da porta para traps do SNMP.

Exemplos

Tarefa Definir o número da porta para traps do SNMP como 162.

Comando: `srmcp -u user1 -p password1 ConfigService set SnmpTrapPort 162`

Tarefa Definir o intervalo de polling para hosts como 70.000.

Comando: `srmcp -u user2 -p password2 ConfigService set hostPollingInterval 70000`

Tarefa Definir o nome da comunidade como GROUP1.

Comando: `srmcp -u user3 -p password3 ConfigService set SnmpCommunityName group1`

Tarefa Definir o intervalo de monitoração para o agente fora da banda como 70.000 milissegundos.

Comando: `srmcp -u user4 -p password4 ConfigService set OutbandAgentMonitorInterval 70000`

Tarefa Definir o valor da descoberta completa para **PollNow**.

Comando: `srmcp -u user4 -p password4 ConfigService set FullAttributeScan PollNow`

Tarefa Definir o valor do URL do IBM Tivoli Storage Resource Manager.

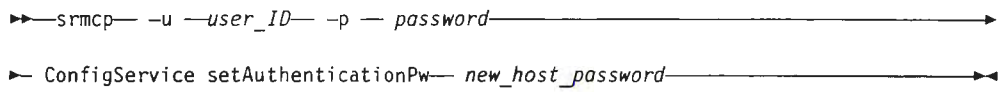
Comando: `srmcp -u user4 -p password4 ConfigService set SRMURL http://mgrvalue.rchland.ibm.com:9530/ITSRM/TivoliSRM.html`

RQS nº 03/2005 - CN
Fls. Nº 1484
3698
Doc.

srmcp ConfigService setAuthenticationPw

O comando **srmcp ConfigService setAuthenticationPw** permite alterar a senha de autenticação do host para o gerenciador, hosts gerenciados e consoles remotos. A senha de autenticação do host é criada quando o IBM Tivoli Storage Area Network Manager é instalado. Este comando pode ser emitido nos computadores do gerenciador, host gerenciado e console remoto.

Sintaxe



Parâmetros

-u *user_ID*
O ID do usuário que emite o comando. Esse parâmetro é obrigatório.

-p *password*
A senha do usuário que emite o comando. Esse parâmetro é obrigatório.

new_host_password
Isso altera a senha de autenticação do host que foi criada quando o IBM Tivoli Storage Area Network Manager foi instalado.

Exemplos

Tarefa Alterar a senha de autenticação do host para **hostpass2**.

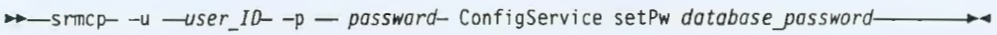
Comando: `srmcp -u user1 -p password1 ConfigService setAthenticationPw hostpass2`

1034

srmcp ConfigService setPw

O comando **srmcp ConfigService setPw** permite que você altere a senha do banco de dados que foi criada quando o IBM Tivoli Storage Area Network Manager foi instalado. Essa **não** é a senha administrativa do DB2 (db2admin). Esse comando pode ser executado somente no computador do gerenciador.

Sintaxe



Parâmetros

-u *user_ID*
O ID do usuário que emite o comando.

-p *password*
A senha do usuário que emite o comando.

database_password
Isso altera a senha do banco de dados do DB2 que foi criada quando o IBM Tivoli Storage Area Network Manager foi instalado. Essa **não** é a senha administrativa do DB2 (db2admin).

Exemplos

Tarefa Alterar a senha do banco de dados para **newpass**.

Comando: `srmcp -u user1 -p password1 ConfigService setPw newpass`

ROS nº 03/2005 - CX
CPMI - CORREIOS
Fls: Nº 1485
Doc. 3698

10321
A.

Apêndice B. Comando do Tivoli NetView

Esta seção descreve o comando do Tivoli NetView, **nvsniffer**. Esse comando é utilizado para descobrir e monitorar os dispositivos iSCSI na rede.

© Copyright IBM Corp 2002, 2003

RQS nº 03/2005
CPMI - CORREIOS
Fls Nº 1486
3698
Doc

nvsniffer

O comando **nvsniffer** é utilizado para descobrir dispositivos iSCSI em nós na rede e para monitorar o status desses dispositivos. Objetos de serviço são criados no banco de dados de objetos para cada dispositivo que seja descoberto em um nó. Os dispositivos de um nó são representados no mapa no nível da interface do nó. Os objetos de dispositivo contêm status e esse status opcionalmente contribui para o status IP geral de um nó. O nó se torna automaticamente um membro do SmartSet de serviço correspondente para cada dispositivo que seja descoberto.

Nota: Esta descrição é um subconjunto dos parâmetros que você pode especificar para o comando **nvsniffer**. Para uma descrição completa do comando **nvsniffer**, consulte o manual *NetView for Windows NT Programmer's Reference*.

Sintaxe

```
►►—nvsniffer— –c —configFile— –r — minutes— –t — numThreads————————►◄
```

Parâmetros

–c *configFile*
Especifique o arquivo de configuração para a descoberta iSCSI.

–r *minutes*
Utilize esta opção para replanejar o **nvsniffer** com as definições e opções atuais. Os minutos especificados indicam com que freqüência o polling é feito. A taxa de polling padrão é a cada 60 minutos. Os valores válidos são de 5 a 44640 minutos (até 31 dias no máximo).

–t *numThreads*
Especifique o número máximo de encadeamentos a serem ativados quando **nvsniffer** for chamado. O intervalo válido é de 1 a 50, inclusive.

Exemplos

Tarefa Executar uma verificação de status em todos os serviços no arquivo de configuração especificado. A verificação de status é feita novamente a cada 120 minutos.

Comando:

```
nvsniffer -c \usr\ov\log\nvsniffer.conf -r 120
```

10319
A.

Apêndice C. Detecção de Problemas

Este apêndice descreve problemas de gerenciamento da SAN que você pode encontrar e como é possível solucioná-los.

É crucial que você instale e mantenha o mais recente nível de manutenção do Tivoli Storage Area Network Manager. Informações e download de manutenção do Tivoli Storage Area Network Manager podem ser obtidos em:

```
http://www.ibm.com/software/support/
```

Antes de entrar em contato com o suporte ao cliente, assegure-se de que tenha instalado a manutenção mais recente do Tivoli Storage Area Network Manager.

Para obter suporte para este ou qualquer outro produto IBM Tivoli, você pode entrar em contato com o IBM Tivoli Customer Support. Consulte "Entrando em Contato com o Suporte ao Cliente" na página vii para obter mais informações.

Verificando Arquivos de Log

O IBM Tivoli Storage Area Network Manager registra ou grava mensagens textuais de eventos do agente, do gerenciador e do console. Você pode verificar os arquivos de log para ver se há erros de eventos nesses componentes a qualquer momento. As tabelas a seguir exibem as localizações padrões dos arquivos de log para todos os componentes da V1.2 e os agentes da V1.1.

Tabela 6. Localizações Padrão dos Arquivos de Log para Componentes da V1.2

Localizações dos Arquivos de Log do Tivoli Storage Area Network Manager V 1.2		
Sistema Operacional	**Componente**	**Localização do Arquivo de Log**
Windows	agente	c:\tivoli\itsanm\agent\log
	gerenciador	c:\tivoli\itsanm\manager\log
	console	c:\tivoli\itsanm\console\log
AIX	agente	/tivoli/itsanm/agent/log
	gerenciador	/tivoli/itsanm/manager/log
Solaris	agente	/tivoli/itsanm/agent/log
Linux (Red Hat e Suse)	agente	/tivoli/itsanm/agent/log

Tabela 7. Localizações Padrão dos Arquivos de Log para Agentes da V1.1

Localizações dos Arquivos de Log do Agente do Tivoli Storage Area Network Manager V 1.1		
Sistema Operacional	**Componente**	**Localização do Arquivo de log**
Windows	agente	c:\tivoli\itsrm\agent\log
AIX	agente	/tivoli/itsrm/agent/log
Solaris	agente	/tivoli/itsrm/agent/log

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1467
3698
Doc

Você pode configurar o tamanho, o tipo, o formato e o locale de seus arquivos de log de mensagens do Tivoli Storage Area Network Manager. Consulte o Apêndice A, "Referência de Comandos", na página 57 para obter mais informações.

Detecção de Problemas de Gerenciamento da SAN

A Tabela 8 descreve os problemas que podem ser encontrados ao executar tarefas de gerenciamento da SAN e como é possível solucioná-los.

Tabela 8. Problemas de Gerenciamento da SAN e Recuperação

Problema	Recuperação
O NetView inicializa com um erro e, em seguida, é encerrado novamente. O serviço do NetView falha ao iniciar novamente após tentativas de reinicializar ou iniciar novamente o serviço.	Entre em contato com o suporte para obter ajuda ao limpar o banco de dados do NetView. Se o banco de dados do NetView for limpo enquanto o Tivoli Storage Area Network Manager estiver em execução, poderá ser necessário reinstalar o NetView.
O NetView pára de funcionar. Os painéis Configurar Manager e Configurar Agente não serão exibidos e as atualizações do log foram interrompidas.	Feche o NetView e, em seguida, reabra-o. Consulte o Apêndice B do *IBM Tivoli Storage Area Network Manager Planning and Installation Guide* para obter mais informações.
Você clica nos itens do menu **SAN** do NetView e nada é exibido.	Assegure-se de que o Serviço SanManagerDaemon esteja sendo executado e, em seguida, clique no item de menu novamente. Se o menu não for exibido, feche o console do NetView; em seguida, reabra-o e clique no item de menu novamente.
Dúvida se o comutador Fibre Channel suporta discovery na banda ou fora da banda.	O site do Tivoli na Web http://www.ibm.com/software/support/ mostra o tipo de suporte para vários comutadores comuns. Entre em contato com o fornecedor se o seu comutador não estiver na lista.
Após executar um poll de discovery ou limpar o histórico, a exibição Exploração do Submapa não é atualizada.	Você pode atualizar o submapa a partir do console. Para atualizar o submapa, clique em **File** → **Refresh Map**. Se você não tiver a opção Refresh Map no menu File, precisará ativar a opção **Advanced Menu**, da seguinte maneira: 1. Clique em **Options** → **Advanced Menu**. 2. Feche o aplicativo Tivoli NetView e inicie novamente. Se o seu submapa não for atualizado após clicar em **Refresh Map**, será necessário limpar o banco de dados do Tivoli NetView, da seguinte maneira: 1. Clique em **Options** → **Server Setup**. 2. Selecione a guia **Databases**. 3. Selecione **Clear Databases** da lista drop-down, no canto superior esquerdo da página de guias. 4. Selecione o botão de opção **Clear All NetView Databases** ou **Clear SNMPCollect Databases**. 5. Clique no botão **OK**.

10317
A-

Tabela 8. Problemas de Gerenciamento da SAN e Recuperação (continuação)

Problema	Recuperação
O Tivoli Storage Area Network Manager não mostra a exibição **Zona** de sua SAN.	Se sua SAN contiver comutadores que suportam o padrão de zoneamento GS-3 Fibre Channel, o Tivoli Storage Area Network Manager recuperará e exibirá as zonas configuradas. Se você não tiver certeza se o seu comutador suporta o padrão de zoneamento GS-3 Fibre Channel, o site do Tivoli na Web http://www.ibm.com/software/support/ mostrará o suporte mais recente para vários comutadores comuns. Se o seu comutador não suportar o padrão de zoneamento GS-3, ainda assim você poderá exibir informações sobre o zoneamento, iniciando um aplicativo do comutador (consulte o Capítulo 4, "Trabalhando com Recursos", na página 41).
A exibição da topologia da SAN no Tivoli NetView não é atualizada quando um dispositivo de rede for removido ou incluído em um host AIX não gerenciado.	Para atualizar o status desse dispositivo na exibição da topologia, você deve executar o Config Manager (cfgmgr) no host AIX não gerenciado ou reinicializar o host AIX não gerenciado. Isso atualiza a exibição da topologia com o status apropriado do dispositivo anexado.
Após configurar um agente fora da banda e definir o nome do usuário e a senha dos comutadores SNMP Brocade fora da banda, a seguinte mensagem de aviso é exibida nos consoles Telnet dos comutadores Brocade para os quais foram inseridas informações corretas de login, uma vez que para cada discovery: `Current Zoning Transaction was aborted. Reason code = Unknown (0)`	Esse é o comportamento esperado e é gerado pelo comutador. Não é necessária nenhuma ação do usuário. O Tivoli Storage Area Network Manager trava a transação de Zoneamento do comutador, antes de ler os dados do zoneamento do comutador. Essa trava é liberada após a operação de leitura ser executada. A mensagem de aviso que indica que a transação de Zoneamento foi liberada é exibida nesse momento, no console do comutador.

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls Nº 1488
Doc. 3698

Tabela 8. Problemas de Gerenciamento da SAN e Recuperação (continuação)

Problema	Recuperação
A topologia exibida no submapa não corresponde à topologia física do loop.	Quando ocorrem determinadas alterações em um loop público de unidades de disco anexadas a um comutador FL_port, o submapa pode não corresponder à topologia de loop real. Isso ocorrerá quando: • Um dispositivo for incluído no loop público. • Um dispositivo for removido do loop público. • Um dispositivo em um loop público não estiver mais respondendo. • Um dispositivo em um loop público que nunca respondeu começar a responder. Sob as condições anteriores, é necessário redefinir o loop, utilizando o *aplicativo de gerenciamento* do comutador. A função de redefinição do loop pode ter os seguintes nomes: • Redefinir loop. • Emitir LIP (Loop Initialization Primitive). • Desativar/Ativar o FL_port. Após a redefinição do loop, o console do Tivoli Storage Area Network Manager será automaticamente atualizado. Se o submapa ainda não refletir com precisão a topologia de loop, clique em **SAN → Configure Manager** e selecione o botão **Poll Now**. Após redefinir o loop público e atualizar a topologia, se esta ainda assim não refletir com precisão o loop, reinicie todos os hosts gerenciados do Windows NT, Windows 2000, Solaris e Linux conectados à malha. Se você estiver executando AIX em um host gerenciado, não será necessário iniciar novamente.
A topologia não é atualizada após um disco ser removido ou incluído em um JBOD.	O comutador pode não gerar um evento para notificar o Tivoli Storage Area Network Manager da remoção ou inclusão. A topologia pode não ser atualizada neste caso. No entanto, o comutador pode enviar uma notificação se estiver executando outra atividade e perceber que o disco foi incluído ou removido. Isso é específico para dispositivos de loop arbitrados.
Impossível iniciar um aplicativo de dispositivo utilizando o Tivoli NetView, pois a opção **Launch Applications** está desativada.	Alguns dispositivos SAN têm aplicativos de gerenciamento, mas não suportam a arquitetura para identificar o nome do aplicativo. Você não pode iniciar esses aplicativos a partir da opção do menu de contexto **Launch Applications**. Se você tiver esse dispositivo, poderá ainda utilizar o Tivoli NetView para iniciar o aplicativo. Consulte "Uma Técnica Alternativa de Início" na página 41 para obter mais informações.

10315
A.

Tabela 8. Problemas de Gerenciamento da SAN e Recuperação (continuação)

Problema	Recuperação
Falha nas operações de backup ou recuperação de dados a partir de um host gerenciado para unidades de fita SCSI locais ou anexadas à SAN.	Dois ou mais comandos SCSI estão sendo enviados simultaneamente para o mesmo dispositivo de mídia removível por diferentes aplicativos do mesmo sistema. Como muitos HBAs enviarão os mesmos comandos SCSI para uma unidade de fita SCSI ou um dispositivo para troca de CD-ROM, que não suporta fila de comandos, causará um erro de comandos sobrepostos e os comandos SCSI falharão. Os aplicativos que estão emitindo os comandos poderão ser finalizados. Por exemplo, o Tivoli Storage Area Network Manager pode estar consultando a unidade de fita ao mesmo tempo em que outro aplicativo do mesmo sistema host está tentando recuperar dados daquela unidade. Para evitar esse problema, não instale o software Tivoli Storage Area Network Manager em sistemas que acessam unidades de fita SCSI locais ou anexadas à SAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1489
Doc. 3698

10314
A-

Apêndice D. Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte um representante IBM local, para obter informações sobre os produtos e serviços atualmente disponíveis em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas o produto, programa ou serviço IBM possa ser utilizado. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados na publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para dúvidas relacionas a informações de DBCS (byte duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie as dúvidas, por escrito, para:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local. A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO-VIOLAÇÃO, MERCADO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias explícitas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. Alterações são periodicamente realizadas nas informações aqui constantes; essas alterações serão incorporadas em novas edições da publicação. A IBM pode a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites não-IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites. Os materiais contidos nesses Web sites não fazem parte deste produto IBM e seu uso é de responsabilidade do Cliente.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1490
Doc. 3698

A IBM pode utilizar ou distribuir as informações fornecidas, da forma que julgar apropriada sem que incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que pretendam obter mais informações com o objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com a:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138/146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, dependendo dos termos e condições apropriadas, incluindo, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito nestas informações e todo o material licenciado disponível para o mesmo são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença do Programa Internacional IBM ou qualquer acordo equivalente.

As informações relativas a produtos não-IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não efetuou testes nestes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade ou qualquer outro requisito relacionado a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Estas informações contêm exemplos de dados e relatórios utilizados em operações diárias de negócios. Para ilustrá-las ao máximo possível, os exemplos incluem nomes de pessoas, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança a esses nomes e endereços utilizados por uma empresa comercial real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX	Magstar
Database 2	MQSeries
DB2	NetView
DB2 Universal Database	Redbooks
Enterprise Storage Server	RISC System/6000
ESCON	RS/6000
IBM	Tivoli
IBMLink	Tivoli Enterprise Console

Lotus, Lotus Notes e Domino são marcas ou marcas registradas da International Business Machines Corporation e da Lotus Development Corporation nos Estados Unidos e/ou em outros países.

Intel e Pentium são marcas ou marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

10312
A.

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada da Open Group nos Estados Unidos e/ou em outros países.

Java e todos os logotipos e marcas baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviços de terceiros.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Apêndice D Avisos 85
Fls. Nº 1491
Nº 3698
Doc.

10311

A.

Glossário

Os termos neste glossário são definidos como pertencentes à biblioteca do IBM Tivoli Storage Area Network Manager. Se você não encontrar o termo necessário, consulte o IBM Software Glossary neste Web site: http://www.ibm.com/ibm/terminology/.

A

agente. Uma entidade que representa um ou mais objetos gerenciados (a) pela emissão de notificações referentes aos objetos e (b) pelo manuseio de solicitações de gerenciadores para operações de gerenciamento para modificar ou consultar os objetos. Consulte também *agente do IBM Tivoli Storage Area Network Manager*.

agente do IBM Tivoli Storage Area Network Manager. O software em um host gerenciado que executa funções locais, como monitoração do sistema de arquivos e discovery em banda. As funções são executadas em coordenação com o gerenciador.

C

coleta de dados. Consulte *discovery*.

console remoto. Um console do IBM Tivoli Storage Area Network Manager que é instalado em uma máquina diferente daquela em que o gerenciador está instalado. Um console remoto permite acessar o IBM Tivoli Storage Area Network Manager de qualquer localização.

D

discovery. O processo de localização de recursos dentro de uma empresa, incluindo a localização do novo local de recursos monitorados que foram movidos. No IBM Tivoli Storage Area Network Manager, o processo detecta recursos de armazenamento lógico e físico no ambiente de armazenamento e suas interconexões (também chamada de topologia). O IBM Tivoli Storage Area Network Manager também coleta atributos de recursos de armazenamento, tais como dados vitais do produto e medidas de capacidade e utilização. Discovery inclui a detecção de alterações na topologia da rede, tal como nós novos e excluídos ou interfaces novas e excluídas. Consulte também *intervalo de discovery*.

discovery em banda. O processo de descobrir informações sobre a SAN, incluindo dados de topologia e atributos, por meio de caminhos de dados do Canal de Fibras. Compare com *discovery fora da banda*.

© Copyright IBM Corp. 2002, 2003

discovery fora da banda. O processo de descobrir informações sobre a SAN, incluindo dados de topologia e dispositivos, sem utilizar os caminhos de dados do Canal de Fibras. Um mecanismo comum para discovery fora da banda é o uso de consultas MIB do SNMP, que são chamadas sobre uma rede TCP/IP. Compare com *discovery em banda*.

E

evento. No ambiente Tivoli, qualquer alteração significativa no estado de um recurso do sistema, recurso da rede ou aplicativo de rede. Um evento pode ser gerado para um problema, para a resolução de um problema ou para a conclusão de uma tarefa com êxito. Exemplos de eventos são: o início e a parada normais de um processo, a finalização anormal de um processo ou a falha de um servidor.

G

gerenciador. O componente do IBM Tivoli Storage Area Network Manager que é instalado em um host e fornece controle centralizado do produto. O gerenciador reúne dados de agentes SNMP e agentes em hosts gerenciados e fornece exibições gráficas de SANs. O gerenciador também pode transferir eventos para o Tivoli Enterprise Console ou um console do SNMP.

GUID (Identificador Globalmente Exclusivo). Um código de 16 bytes que identifica uma interface para um objeto em todos os computadores e redes. O identificador é exclusivo porque contém uma data e hora e um código com base no endereço da rede que é conectado à placa da interface da LAN do computador host.

H

host. Um computador que é conectado a uma rede (como a Internet ou uma SAN) e fornece um ponto de acesso a essa rede. Além disso, dependendo do ambiente, o host pode fornecer controle centralizado da rede. O host pode ser um cliente, um servidor, um cliente e um servidor, um gerenciador ou um host gerenciado.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 1492
Doc: 3698

host gerenciado. Um host que é gerenciado pelo IBM Tivoli Storage Area Network Manager. O host tem um agente do IBM Tivoli Storage Area Network Manager instalado e ativo nele. Os hosts gerenciados são utilizados para discovery em banda da SAN e para gerenciamento do sistema de arquivos.

I

intervalo de discovery. A freqüência na qual as informações de topologia e atributos são reunidas pelos agentes do IBM Tivoli Storage Area Network Manager e enviadas ao gerenciador. O intervalo de discovery é definido por um planejamento para que ocorra periodicamente ou em períodos específicos. Discovery também pode ocorrer em outros momentos, como quando disparada por um evento a partir da opção SAN.

L

LUN. Consulte *número da unidade lógica.*

LUN (Número da Unidade Lógica). Um identificador utilizado em um barramento SCSI para diferenciar entre dispositivos (unidades lógicas) com o mesmo ID do SCSI.

N

nome da comunidade. A parte de uma mensagem do SNMP que representa um nome parecido com uma senha e que é utilizada para autenticar a mensagem do SNMP.

T

topologia. A disposição física e lógica de dispositivos em uma SAN (Rede da Área de Armazenamento). A topologia pode ser exibida graficamente, mostrando os dispositivos e suas interconexões.

10309

Índice Remissivo

A

agentes
  configurando 16
  iniciando no AIX 15
  iniciando no Solaris 15
  iniciando no Windows 15
  verificando arquivos de log 77
ajuda on-line
  exibindo 22
arquivo de propriedades do usuário
  definir valores da propriedade 12, 70
  exibir valor do nome da propriedade 68
  exibir valores em 12, 67
arquivos de log
  verificando 77

C

comando nvsniffer 40, 76
comando srmcp ConfigService display 67
comando srmcp ConfigService get 68
comando srmcp ConfigService help 69
comando srmcp ConfigService set 70
comando srmcp ConfigService setAuthenticationPw 72
comando srmcp ConfigService setPw 73
comando srmcp log get 62
comando srmcp log help 63
comando srmcp log set 64
comandos
  definindo ambiente para emissão 60
  inserindo 60
  lendo diagramas de sintaxe 57
  nvsniffer 76
  referência 57
  srmcp ConfigService display 67
  srmcp ConfigService get 68
  srmcp ConfigService help 69
  srmcp ConfigService set 70
  srmcp ConfigService setAuthenticationPw 72
  srmcp ConfigService setPw 73
  srmcp log get 62
  srmcp log help 63
  srmcp log set 64
  tipos de 57
comandos de Service Manager 66
  exibindo ajuda para 69
  srmcp ConfigService display 67
  srmcp ConfigService get 68
  srmcp ConfigService help 69
  srmcp ConfigService set 70
  srmcp ConfigService setAuthenticationPw 72
  srmcp ConfigService setPw 73
comandos de serviço de registro 61
configurando
  agente do IBM Tivoli Storage Area Network Manager 16
  agente SNMP 16
  arquivos de propriedades do usuário 12
  destino do evento 19
  EDFI 44
  log de mensagens 11
conjuntos de regras (EDFI)
  carregando 47
  exibindo 47
  selecionando 47
contato por e-mail vi

D

DB2
  suportado 10
diagrama de sintaxe
  visão geral 57
discovery
  completa, definindo valor para 70
  descrição de 4
  planejando polling para 21
discovery fora da banda
  alternar suporte para 18
discovery na banda
  alternar suporte para 18
dispositivos
  estados de conexão, definido 29
  exibindo conexões do dispositivo 29
  exibindo propriedades 29
  iniciando aplicativos do dispositivo 41
  limpando histórico do status 36
  reconstruindo exibições de submapas 36
  símbolos, alterando rótulos e ícones 32
  status do símbolo, visão geral 33

E

EDFI (Detecção de Erros e Isolamento de Falhas)
  carregando um conjunto de regras 47
  configurando 44
  eventos 46, 48
  exibindo um conjunto de regras 47
  identificando hardware com defeito na exibição da topologia 53
  início 45
  localizando um erro na exibição da topologia 50
  notificações de erros
    exibindo 48
    limpando 54
  parando 45
EDFI (Detecção de Erros e Isolamento de Falhas) *(continuação)*
  selecionando um conjunto de regras 47
  visão geral 44
eventos
  configurando destino 19
  EDFI 46, 48
  exibir no banco de dados de eventos do NetView 43
exibição central do dispositivo
  exibindo hosts associados 27
  exibindo LUNs associadas 27
  exibindo sistema operacional do host 27
  exibindo sistemas de arquivos do host 27
exibição central do host
  exibir 26
  exibir dispositivo de armazenamento em disco do volume lógico 26
  exibir sistema operacional do host 26
  exibir sistemas de arquivos do host 26
Exibição da SAN
  mostrar exibição da topologia 23
  mostrar exibição das zonass 23
exibição das zonas
  exibir 23
exibindo
  arquivo de propriedades do usuário 12
  o log de mensagens 11

G

gerenciador
  arquivo de log 77
  descrição de 3
Gerenciamento da SAN
  problemas, detecção de problemas 78
  tarefas do administrador 8

H

hosts
  descrição de 4
hosts gerenciados
  descrição de 4

I

IBM Tivoli Storage Area Network Manager
  alterando senha do banco de dados 73
  início 15
informações sobre manutenção
  IBM Tivoli Storage Area Network Manager 77

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1493
Doc. 3698

início
agentes 15
em AIX 15
em Solaris 15
Windows 15
EDFI 45
interface do Tivoli Storage Resource Manager 12
interface com o usuário da Web
iniciando a partir do console do Tivoli NetView 13
interfaces para o Tivoli Storage Area Network Manager 8

L

limpando uma notificação de erro 54
localizando um erro na exibição da topologia (EDFI) 50

M

manuais
feedback v, vi
on-line v, vi
solicitando v, vi

O

opções
informações de conta administrativa do Brocade 17
URL para suporte 18

P

polling
considerações sobre desempenho 21
informações sobre a SAN 21
publicações
feedback v, vi
on-line v, vi
solicitando v, vi

R

rede
exibir Rede da Área de Armazenamento 22
iniciando aplicativos do dispositivo 41
mostrar exibição de exploração do submapa 22
Rede da Área de Armazenamento
exibição gráfica 22
registro de mensagens
comandos de configuração 11, 61
definir propriedades do log de mensagens 11, 64
exibir ajuda da linha de comando 63
propriedades, exibição 62
visão geral 11

S

segurança, sistema de arquivos 11
senha de autenticação do host
alterando 72
setenv
definindo para emitir comandos 60
símbolo de dispositivo
filtrando com base no status 37
propagação do status padrão 34
visão geral do status 33
sistemas de arquivos
segurança para 11
SNMP
utilizando para gerenciar eventos 43
solução de problemas
problemas de gerenciamento da SAN 78
suporte a Internet SCSI
iniciando descoberta no NetView 38
parando descoberta no NetView 40
reprogramando polling 40
visão geral 6
Suporte ao Cliente vii
Suporte ao Cliente IBM vii
Suporte de comutador para discovery na banda 25

T

Tivoli Event Browser
exibir banco de dados de eventos do NetView 43
Tivoli NetView
arquivo de log 77
Tivoli Storage Resource Manager, iniciando a interface 12
topologia
exibir 5, 24

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 1494
Doc 3698

10306
A.

Manual 10

IBM Tivoli
Storage Area Network Manager
Guia do Planejamento e Instalação
Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1495
Doc 3698

10305
A.

IBM

IBM Tivoli Storage Area Network Manager

Guia de Planejamento e Instalação

Versão 1 Release 2

RQS nº 03/2008 - CN
CPMI - CORREIOS
Fls. Nº 1496
3510-7575-01
Nº Doc: 3698

IBM Tivoli Storage Area Network Manager

Guia de Planejamento e Instalação

Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
1497
Fls- Nº
3698
Doc.
S517-7575-01

10303
CA.

Nota!
Antes de utilizar estas informações e o produto a que se referem, assegure-se de ler as informações gerais no Apêndice E, "Avisos", na página 227.

Segunda Edição (Abril de 2003)

Esta edição se aplica à versão 1, release 2, modificação 0 do IBM Tivoli Storage Area Network Manager (números de programa 5698-SRE e 5698-SRS) e a todos os releases subseqüentes, até que o contrário seja indicado em novas edições.

As alterações desde a edição anterior são marcadas com uma barra vertical (|) na margem esquerda. Assegure-se de que está utilizando a edição correta para o nível do produto.

Solicite publicações por meio de seu representante de vendas ou pela filial que atende a sua localidade.

O seu feedback é importante para ajudar a fornecer informações mais precisas e de melhor qualidade. Se você tiver comentários sobre esse manual ou qualquer outra documentação do IBM Tivoli Storage Area Network Manager, consulte "Entrando em Contato com o Suporte ao Cliente" na página x.

© Copyright International Business Machines Corporation 2002, 2003. Todos os direitos reservados.

10302

A.

Índice

Prefácio vii
Quem Deve Ler Este Guia vii
Publicações vii
Publicações do IBM Tivoli Storage Area Network Manager vii
Publicações Relacionadas viii
Acessando Publicações On-line viii
Solicitando Publicações ix
Fornecendo Feedback sobre Publicações x
Acessibilidade x
Entrando em Contato com o Suporte ao Cliente . . x
Relatando um Problema xi
Convenções Utilizadas neste Manual xi
Convenções Tipográficas xi

Resumo das Alterações para o IBM Tivoli Storage Area Network Manager Versão 1 xiii
Alterações Técnicas para a Versão 1 Release 2 – Abril de 2003 xiii

Capítulo 1. Apresentando o IBM Tivoli Storage Area Network Manager. 1
Gerenciamento da Rede da Área de Armazenamento 2
Descoberta 2
Descoberta Completa 3
Descoberta de SCSI na Internet 4
Exibições da Topologia 4
Eventos do SNMP 4
Detecção de Erros e Isolamento de Falhas . . . 4
Suporte à Internet SCSI 5
Interfaces para o Tivoli Storage Area Network Manager 8
Integrando o IBM Tivoli Storage Area Network Manager à Solução de Gerenciamento SNMP . . . 8

Capítulo 2. Planejando a Instalação . . . 9
Requisitos do Sistema para o Tivoli Storage Area Network Manager 10
Requisitos de Armazenamento 10
Requisitos do Gerenciador (Windows 2000). . . 10
Requisitos do Gerenciador (AIX) 11
Requisitos do Console Remoto do IBM Tivoli Storage Area Network Manager 12
Requisitos do Agente 12
Considerações sobre Compatibilidade 13
Limitações 13
Outros Suportes 14
Ambiente da SAN 14
Visão Geral das Etapas de Instalação para Instalar o IBM Tivoli Storage Area Network Manager 14
Etapas de Instalação para um Gerenciador do Windows 16
Etapas de Instalação para um Gerenciador do AIX 16
Fazendo Upgrade do IBM Tivoli Storage Area Network Manager 17
Alterações para o IBM Tivoli Storage Area Network Manager Versão 1.2 17

Capítulo 3. Preparando-se para a Instalação (Gerenciador do Windows) . 19
Etapa 1: Verificar Itens Necessários 19
Etapa 2: Verificar o Nome do Computador 21
Etapa 3: Alterar o Arquivo HOSTS 22
Etapa 4: Instalar o DB2 22
Fazendo o Upgrade do DB2 com o FixPak 8 . . 28
Fazendo o Upgrade dos Drivers JDBC do DB2 para a Versão 2 29
Etapa 5: Instale o Serviço SNMP 29
Verificando o Nome da Comunidade SNMP . . 32

Capítulo 4. Preparando-se para a Instalação (Gerenciador do AIX). . . . 35
Etapa 1: Verificar Itens Necessários 35
Etapa 2: Verificar o Nome do Computador 37
Etapa 3: Instalar o DB2 39
Fazendo o Upgrade do DB2 com o FixPak 8 . . 46
Criando uma Instância do Banco de Dados e o Servidor de Administração 47
Atualizando a Variável de Ambiente EXTSHM . 57
Verificando o DB2 57

Capítulo 5. Instalando o Gerenciador do Windows 59
Instalando o Gerenciador 62
Iniciando e Parando o Gerenciador 76
Verificando os Arquivos de Log 77

Capítulo 6. Instalando o Gerenciador do AIX 79
Instalando o Gerenciador do AIX 80
Iniciando e Parando o Gerenciador 82
Verificando os Arquivos de Log 82

Capítulo 7. Instalando o Agente no Host Gerenciado 83
Instalando o Agente do IBM Tivoli Storage Area Network Manager no Windows 2000 ou NT . . . 83
Iniciando e Encerrando o Agente no Windows. . 92
Instalando o Agente no Solaris 92
Iniciando e Encerrando o Agente no Solaris . . 92
Instalando o Agente no AIX 92
Iniciando e Encerrando o Agente no AIX . . . 93
Instalando o Agente no Linux 93
Iniciando e Encerrando o Agente no Linux . . . 93

© Copyright IBM Corp. 2002, 2003

POS-PF 03/2005 - CPMI - 1498
Doc 3698

Verificando os Arquivos de Log 93

Capítulo 8. Instalando o Console Remoto do IBM Tivoli Storage Area Network Manager 95
Antes de Instalar o Console Remoto 95
Instalando o Console Remoto 96
Iniciando e Parando o Console Remoto. 104
Verificando os Arquivos de Log 105

Capítulo 9. Configurando o IBM Tivoli Storage Area Network Manager . . . 107
Controlando e Filtrando Eventos 107
Opções de Configuração. 108
Configurando Dispositivos e Programas para Enviar Todos os Traps SNMP ao Console Tivoli NetView 108
Configurando Dispositivos para Enviar Traps ao IBM Tivoli Storage Area Network Manager . . 110
Configurando Dispositivos para Enviar Traps ao IBM Tivoli Storage Area Network Manager e ao Console SNMP 110
Configurando os Agentes Fora de Banda 112
Configurando o Arquivo MIB no Tivoli NetView 113
Configurando o IBM Tivoli Storage Area Network Manager para Enviar Eventos 113
Configurando Dispositivos para Enviar Eventos ao Tivoli Enterprise Console 116
Configurando o Tivoli Enterprise Console para Receber Eventos do IBM Tivoli Storage Area Network Manager 116
Eventos do IBM Tivoli Storage Area Network Manager 118
Configurando o IBM Tivoli Storage Area Network Manager para a Descoberta de iSCSI 118
Arquivos MIB iSCSI 118
Ativando a Descoberta da Rede IP 119
Iniciando a Descoberta iSCSI 121
Parando a Descoberta iSCSI 122
Configurando o IBM Tivoli Storage Area Network Manager para EDFI 123
Carregando um Conjunto de Regras. 123
Iniciando e Parando a EDFI 124
Selecionando um Conjunto de Regras 126
Relatório de Eventos EDFI 126
Configurando uma SAN sem Hosts Gerenciados 127

Capítulo 10. Fazendo Upgrade do IBM Tivoli Storage Area Network Manager . 129
Fazendo o Upgrade do Gerenciador do Windows 129
Fazendo o Upgrade do Console Remoto 139
Fazendo o Upgrade dos Agentes 146
Fazendo o Upgrade do Agente no Windows . . 146
Fazendo o Upgrade do Agente no AIX 151
Fazendo o Upgrade do Agente no Solaris . . . 151

Capítulo 11. Instalando o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager. 153
Instalando o Pacote de Idiomas no Gerenciador do Windows. 153
Instalando o Pacote de Idiomas no Gerenciador do AIX 162
Instalando o Pacote de Idiomas no Console Remoto 163
Instalando o Pacote de Idiomas no Host Gerenciado 163
Instalando o Pacote de Idiomas no Windows 163
Instalando o Pacote de Idiomas no AIX. . . . 164
Instalando o Pacote de Idiomas no Solaris. . . 164
Instalando o Pacote de Idiomas no Linux . . . 164
Removendo a Instalação do Pacote de Idiomas . . 165

Capítulo 12. Removendo a Instalação do IBM Tivoli Storage Area Network Manager 171
Desinstalando o Gerenciador no Windows. . . . 171
Removendo a Instalação do Pacote GUID Tivoli 177
Desinstalando o Gerenciador no AIX 177
Removendo a Instalação do Console Remoto do IBM Tivoli Storage Area Network Manager . . . 178
Desinstalando os Agentes 182
Desinstalando o Agente no Windows 182
Desinstalando o Agente no AIX ou Solaris. . . 185
Desinstalando o Agente com Linux 186
Removendo a Instalação do DB2 186
Desinstalando o DB2 no Windows 186
Desinstalando o DB2 no AIX 187

Apêndice A. Instalação Silenciosa do IBM Tivoli Storage Area Network Manager 189
Instalando o Gerenciador 189
Como Instalar o Gerenciador 192
Instalando o Agente 193
Como Instalar o Agente 194
Instalando o Console Remoto 195
Como Instalar o Console Remoto. 198
Desinstalando o IBM Tivoli Storage Area Network Manager 198
Removendo a Instalação do Gerenciador . . . 198
Desinstalando Console Remoto 198
Desinstalando os Agentes 198

Apêndice B. Sugestões e Dicas . . . 201
Dicas sobre Execução com o DB2. 201
Configurando o Banco de Dados DB2 201
Gerenciando os Logs de Transação 202
Utilizando o DB2 no Windows 203
Utilizando o DB2 no AIX 204
Verificando Nomes de Host Completos. 204
Sistemas Windows 2000 205
Sistemas Windows NT 205
Sistemas AIX 205
Sistemas Solaris 206
Sistemas Linux 206
Alterando o Arquivo HOSTS 206
Verificando um Endereço IP Estático. 207
Alterando o Nome da Comunidade SNMP . . . 208

Dicas sobre Execução com o Tivoli NetView . . . 209
Como Ativar um Aplicativo a partir do Console Remoto 209
Como Verificar o Daemon do NetView 209
Informações Adicionais 210
Como o Tivoli Storage Area Network Manager Utiliza Eventos em Banda e Traps SNMP Fora de Banda 210
Informações Coletadas com o Uso de Comutadores e HBAs de Fornecedores 212
| Ativando a MIB de Gerenciamento FC 213
| Classes de Eventos e Atributos do Tivoli Enterprise
| Console 213

Apêndice C. Detecção de Problemas 221

Detectando Problemas do Tivoli NetView 221
Detectando Problemas do IBM Tivoli Storage Area Network Manager 221

Apêndice D. Acessibilidade 225
Navegando pela Interface Utilizando o Teclado . . 225
Ampliando o que É Exibido na Tela 225

Apêndice E. Avisos 227
Marcas 228

Glossário 231

Índice Remissivo 233

10300
RQS nº 03/2005 - CN
CPMI - CORREIOS
1499
Fls Nº
3698
Doc.

1029

Título	Número de Ordem
IBM Tivoli Storage Area Network Manager Publications CD-ROM	SCD7-0463

As publicações também estão disponíveis no Web site de publicações Tivoli:
`http://publib.boulder.ibm.com/tividd/td/tdprodlist.html`

Publicações Relacionadas

A tabela a seguir lista publicações relacionadas.

Título	Número de Ordem
IBM Tivoli Storage Area Network Manager: A Practical Introduction (Redbook)	SG24–6848
Introduction to Storage Area Network, SAN	SG24–5470
Designing an IBM Storage Area Network	SG24–5758
NetView for Windows User's Guide	SC31–8888
NetView for Windows NT Programmer's Reference	SC31–8890
IBM Tivoli Enterprise Console: Guia do Usuário	GC32–0667
IBM Enterprise Storage Server	SG24–5465
iSCSI: The Universal Storage Connection by John L. Hufferd	

Para obter mais informações sobre Redbooks, consulte

http://www.redbooks.ibm.com/redbooks.

O *Tivoli Software Glossary* inclui definições para muitos dos termos técnicos relacionados ao software Tivoli. O *Tivoli Software Glossary* está disponível, somente em inglês, no seguinte Web site:

http://publib.boulder.ibm.com/tividd/glossary/termsmst04.htm.

Acessando Publicações On-line

Você pode acessar as publicações no Tivoli Information Center a partir do seguinte Web site de Suporte ao Cliente:

http://www-3.ibm.com/software/tivoli/library/

O Tivoli Information Center contém a versão mais recente dos manuais da biblioteca de produtos nos formatos PDF ou HTML, ou em ambos. Os documentos traduzidos também estão disponíveis para alguns produtos.

Nota: Se você imprimir documentos em PDF em papel que não seja do tamanho carta, selecione a caixa de opções **Ajustar à página**, no diálogo **Impressão no Adobe Acrobat**. Essa opção estará disponível quando você clicar em **Arquivo → Imprimir**. A opção **Ajustar á página** assegura que as dimensões totais de uma página do tamanho carta sejam impressas no papel que você está utilizando.

ROS nº 03/2003 - CN
CPMI - CORREIOS
1300
Fls Nº
3698
Doc.

Prefácio

O IBM Tivoli Storage Area Network Manager gerencia todos os seus dispositivos em uma SAN (Rede de Área de Armazenamento). As capacidades incluem discovery, monitoração, disponibilidade e gerenciamento de eventos. O *IBM Tivoli Storage Area Network Manager: Guia do Usuário* descreve como gerenciar os recursos na rede de área de armazenamento.

Este manual fornece informações para ajudá-lo a desempenhar as seguintes tarefas:

- Planejar a instalação do IBM Tivoli Storage Area Network Manager
- Instalar o IBM Tivoli Storage Area Network Manager
- Configurar o IBM Tivoli Storage Area Network Manager

Quem Deve Ler Este Guia

Este manual inclui instruções para que instaladores e administradores de SAN planejem, instalem e configurem o IBM Tivoli Storage Area Network Manager. Esses instaladores e administradores devem estar familiarizados com o seguinte:

- Procedimentos gerais para a instalação de softwares em um sistema Windows
- Conceitos da SAN
- DB 2 (Database 2)
- Conceitos de SNMP (Simple Network Management Protocol)
- Tivoli NetView

Depois de instalar o IBM Tivoli Storage Area Network Manager, você deve ler o *IBM Tivoli Storage Area Network Manager: Manual do Usuário*. Ele o ajudará a obter noções básicas sobre o uso do produto.

Publicações

Esta seção lista as publicações na biblioteca do IBM Tivoli Storage Area Network Manager e quaisquer outros documentos relacionados. Também descreve como acessar publicações Tivoli on-line, como solicitar solicitar essas publicações Tivoli e como fazer comentários sobre elas.

Publicações do IBM Tivoli Storage Area Network Manager

A tabela a seguir lista as publicações do IBM Tivoli Storage Area Network Manager.

Título da Publicação	Número de Ordem
IBM Tivoli Storage Area Network Manager: Guia do Usuário	S517-7576
IBM Tivoli Storage Area Network Manager Planning and Installation Guide	SC23-4697
IBM Tivoli Storage Area Network Manager Messages	SC32-0953

A biblioteca do Tivoli Storage Area Network Manager em todos os idiomas está disponível no seguinte CD:

© Copyright IBM Corp. 2002, 2003

Solicitando Publicações

É possível solicitar várias publicações on-line do Tivoli no seguinte Web site:

`http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi`

Também pode solicitar por telefone, ligando para um destes números:

- Nos Estados Unidos: 800–879–2755
- No Canadá: 800–426–4968

10297
A-

RQS nº 03/2005 - CN
CPMI - CORREIOS
1501
Fls Nº
3698
Doc.

Em outros países, consulte o seguinte Web site para obter uma lista de números de telefone:

`http://www.ibm.com/software/tivoli/order-lit/`

Fornecendo Feedback sobre Publicações

Se você tiver comentários ou sugestões sobre os produtos e a documentação do Tivoli, envie um e-mail para pubs@tivoli.com ou preencha a pesquisa de feedback do cliente no seguinte Web site:

`http://www.ibm.com/software/tivoli/contact.html`

Acessibilidade

Os recursos de acessibilidade ajudam um usuário que tem uma deficiência física, como por exemplo mobilidade restrita ou visão limitada, a utilizar produtos de software com êxito. Com este produto, você pode utilizar tecnologias de apoio para ouvir e navegar na interface. Também é possível utilizar o teclado em vez do mouse para operar todos os recursos da interface gráfica com o usuário.

Para obter informações adicionais, consulte Apêndice D, "Acessibilidade", na página 225.

Entrando em Contato com o Suporte ao Cliente

Para obter suporte referente a esse ou qualquer outro produto Tivoli, você pode entrar em contato com o suporte ao cliente IBM de uma das seguintes maneiras:

- Visite o site de suporte técnico do IBM Tivoli Storage Area Network Manager na Web em http://www.ibm.com/software/support/.
- Submeta eletronicamente um PMR (Registro de Gerenciamento de Problemas) em **IBMSERV/IBMLINK**. É possível acessar o IBMLINK no endereço http://www2.ibmlink.ibm.com.
- Envie um PMR eletronicamente no endereço http://www.ibm.com/software/sysmgmt/products/support/. Consulte "Relatando um Problema" na página xi para obter detalhes.

Clientes nos Estados Unidos também podem telefonar para 1-800-IBM-SERV (1-800-426-7378).

Os clientes internacionais devem consultar o Web site para obter os números de telefone de suporte ao cliente.

Clientes com deficiência auditiva devem visitar o Web site do TDD/TTY Voice Relay Services and Accessiblity Center no endereço http://www.ibm.com/able/voicerelay.html.

Você também pode ler o *IBM Software Support Handbook*, que está disponível em nosso Web site no endereço http://techsupport.services.ibm.com/guides/handbook.html.

Ao entrar em contato com o suporte ao cliente, esteja preparado para fornecer informações de identificação de sua empresa, para que a equipe de suporte possa ajudá-lo prontamente. As informações de identificação da empresa também podem ser necessárias para acessar diversos serviços on-line disponíveis no Web site.

10295
A.

O site de suporte da Web oferece informações completas, incluindo um guia para serviços de suporte (o IBM Software Support Handbook); FAQs (Perguntas mais Freqüentes); e a documentação de todos os produtos de software IBM, incluindo Notas de Release, Redbooks e Documentos Técnicos. A documentação para alguns releases do produto está disponível nos formatos PDF e HTML. Documentos traduzidos também estão disponíveis para alguns releases do produto.

Todas as publicações do Tivoli estão disponíveis para download eletrônico ou podem ser solicitadas no IBM Publications Center:http://www-3.ibm.com/software/tivoli/library/

Estamos muito interessados em saber sobre sua experiência com os produtos e a documentação do Tivoli. Suas sugestões de melhorias também são bem-vindas. Se tiver comentários ou sugestões sobre nossa documentação, preencha a pesquisa de feedback do cliente em

`http://www-3.ibm.com/software/sysmgmt/products/support/Tivoli_Escalation_Process.html`

Relatando um Problema

Tenha as seguintes informações prontas ao comunicar um problema:

- Os números de versão, release, modificação e nível de serviço do IBM Tivoli Storage Area Network Manager.
- O número do protocolo de comunicação (por exemplo, TCP/IP), da versão e do release que você está utilizando.
- A atividade que você estava executando quando o problema ocorreu, listando as etapas seguidas antes de o problema ocorrer.
- O texto exato de quaisquer mensagens de erro.

Convenções Utilizadas neste Manual

Este manual utiliza diversas convenções para termos e ações especiais, além de caminhos e comandos dependentes do sistema operacional.

Convenções Tipográficas

As seguintes convenções de tipos são utilizadas neste manual:

Negrito

- Comandos em minúsculas ou combinados com maiúsculas e minúsculas que aparecem com o texto
- Opções de comando que aparecem com o texto
- Sinalizadores que aparecem com o texto
- Elementos da interface gráfica com o usuário (exceto títulos de janelas e caixas de diálogo)
- Nomes te chaves

Itálico

- Variáveis
- Valores que você deve fornecer
- Novos termos
- Palavras e frases que estão enfatizadas
- Títulos de documentos

`Espaçamento Fixo`

- Comandos e opções de comandos nos exemplos
- Flags exibidos em uma linha separada
- Saída e exemplos de código

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls Nº 1502
Nº Doc 3698

- Texto da mensagem
- Nomes de arquivos e diretórios
- Cadeias de texto que você deve digitar, quando exibidas no texto
- Nomes de métodos e classes Java
- Marcações HTML e XML também são exibidas `desta forma`, com fonte de `espaço fixo`

São utilizadas estas convenções para notação de sintaxe:

- <> (símbolos menor que, maior que) são utilizados para indicar um valor de variável. Não digite os símbolos <>.
- # é o prompt para o usuário root.
- Letras maiúsculas e minúsculas são consideradas. Digite os comandos exatamente como aparecem.

Resumo das Alterações para o IBM Tivoli Storage Area Network Manager Versão 1

Esta seção resume as alterações que foram feitas no produto e nesta publicação.

Alterações Técnicas para a Versão 1 Release 2 – Abril de 2003

As seguintes alterações foram feitas no produto para esta edição:

EDFI (Detecção de Erro e Isolamento de Falha)
A função EDFI fornece ajuda com determinação de problemas em links de interconexão SAN Fibre Channel. A EDFI utiliza análise de falhas previstas e fornece capacidades de isolamento de falhas que permitem identificar e tomar a ação apropriada para componentes que possam estar falhando.

Embedded WebSphere Application Server – Express, Versão 5.0
A instalação do IBM Tivoli Storage Area Network Manager inclui a versão incorporada do WebSphere Application Server – Express. Uma instalação separada do WebSphere não é mais necessária.

Suporte a iSCSI (Internet SCSI)
Internet SCSI é um padrão proposto pelo mercado que permite que sistemas de computadores centrais executem operações em bloco de entrada/saída de dados com diversos dispositivos. Os dispositivos de destino podem incluir dispositivos de disco e fita e dispositivos de armazenamento. O protocolo Internet SCSI define um meio de ativar os aplicativos de armazenamento de blocos pelas redes TCP/IP. Você pode descobrir dispositivos que utilizam o protocolo de rede de armazenamento iSCSI por meio do Tivoli NetView.

Suporte do sistema operacional AIX para o gerenciador
O IBM Tivoli Storage Area Network Manager (componente do gerenciador) é suportado no AIX 5.1. Esse suporte não inclui o suporte Tivoli NetView no AIX. Se desejar ver a exibição da GUI no IBM Tivoli Storage Area Network Manager, instale o console remoto no Windows 2000 ou Windows XP.

Suporte ao Console Remoto no Windows XP
O console remoto do IBM Tivoli Storage Area Network Manager agora é suportado no Windows XP. O Tivoli NetView 7.1.3 é requerido para suportar o Windows XP.

O suporte do sistema operacional foi adicionado para os hosts gerenciados:
- Host gerenciado no AIX 5.2
- Host gerenciado no Linux Redhat Advanced Server versão 2.1
- Host gerenciado no SuSE Linux Enterprise Server 7.0

O suporte ao sistema operacional foi eliminado para o seguinte componente:
Para hosts gerenciados no AIX 4.3.3 (para a versão 1.1), o suporte foi eliminado. O host gerenciado, release 1, ainda é compatível com um gerenciador do release 2.

Endereços IP dinâmicos para hosts gerenciados e consoles remotos
É possível especificar endereços IP dinâmicos em vez de endereços IP estáticos para hosts gerenciados e consoles remotos. O gerenciador ainda exige um endereço IP estático.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 1503
3698
Doc

Identificação da SAN
O IBM Tivoli Storage Area Network Manager agora exibe o nome da SAN ao qual um objeto está conectado.

Classes de Eventos Adicionais do Tivoli Enterprise Console
O IBM Tivoli Storage Area Network Manager fornece classes de eventos adicionais para o Tivoli Enterprise Console que permitem filtrar eventos facilmente com base no tipo de evento. Consulte "Classes de Eventos e Atributos do Tivoli Enterprise Console" na página 213.

Suporte à chave Cisco Série MDS 9000
O IBM Tivoli Storage Area Network Manager aprimorou a compatibilidade para a chave Cisco Série MDS 9000. O Tivoli NetView exibe os números das portas em um formato de SSPP, em que SS é o número do slot e PP é o número da porta. O item do menu Ativar Aplicativo está disponível para a chave Cisco. Quando Ativar Aplicativo é selecionado, o aplicativo Cisco Fabric Manager é iniciado.

Versão do Agente
Um agente do IBM Tivoli Storage Area Network Manager AIX 4.3.3 release 1 em um host gerenciado pode coexistir com um gerenciador do release 2. O IBM Tivoli Storage Area Network Manager acompanha as diferenças de funcionalidade entre um agente do release 1 e um agente do release 2 e toma a ação apropriada com base nessas informações. Não é possível ter um agente do release 1 e um agente do release 2 no mesmo host gerenciado (somente um agente por host gerenciado). O agente do release 1 não suportará a nova função (por exemplo, EDFI ou iSCSI).

Novos Ícones para Entrada Manual
Quando executada a entrada manual em dispositivos desconhecidos, os seguintes ícones estarão disponíveis:
- ESS
- Controlador de Volume SAN

Outras Alterações
- O MQSeries foi removido deste release.
- Feito o upgrade do Tivoli NetView para a versão 7.1.3.
- Foi feito o upgrade de JRE 1.3.0 para JRE 1.3.1.
- A instalação silenciosa do IBM Tivoli Storage Area Network Manager é suportada. Consulte Apêndice A, "Instalação Silenciosa do IBM Tivoli Storage Area Network Manager", na página 189.
- O estado suspenso foi removido do console. Anteriormente o estado suspenso era utilizado para notificar o usuário que o dispositivo estava em um estado crítico. O estado suspenso permanecia até que o dispositivo retornasse ao estado crítico ou o usuário limpasse o estado.

10291
A-

Capítulo 1. Apresentando o IBM Tivoli Storage Area Network Manager

O Tivoli Storage Area Network Manager o ajuda a gerenciar seus recursos fornecendo capacidades de descoberta e gerenciamento de recursos de rede.

A Figura 1 mostra como o Tivoli Storage Area Network Manager pode gerenciar todos os seus recursos de armazenamento. Isso inclui dispositivos que estão conectados a sistemas host por meio de hubs, pontes, comutadores, roteadores, gateways e direcionadores com base em fibra ótica. O Tivoli Storage Area Network Manager também pode gerenciar qualquer host com um agente que não esteja conectado à SAN.

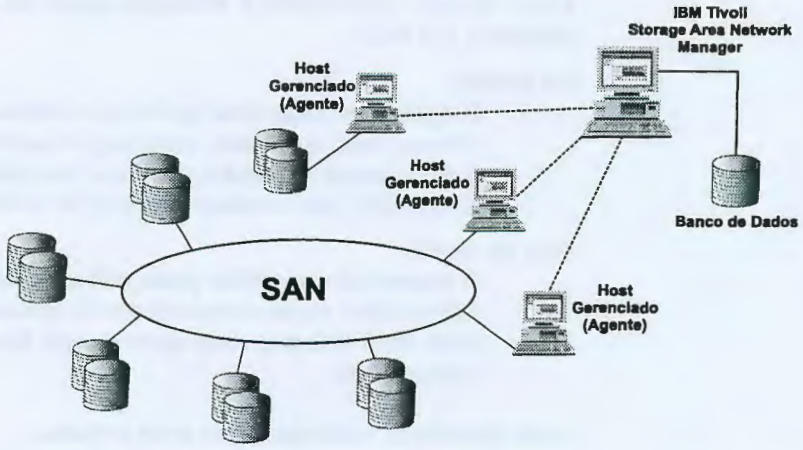


Figura 1. O IBM Tivoli Storage Area Network Manager em um Ambiente de Rede de Área de Armazenamento

Com o Tivoli Storage Area Network Manager, um sistema age como o gerenciador e um ou mais outros sistemas são os hosts gerenciados:

Gerenciador

O gerenciador faz o seguinte:

- Reúne dados dos agentes em hosts gerenciados, como descrições de SANs (Redes da Área de Armazenamento), LUNs (Números de Unidade Lógica) e informações sobre o sistema de arquivos e o host.
- Fornece exibições gráficas da topologia da SAN.
- Gera eventos SNMP (Simple Network Management Protocol) quando uma alteração for detectada na estrutura da SAN.
- Transfere eventos para o Tivoli Enterprise Console ou um console do SNMP.

Hosts gerenciados

Um agente reside em cada host gerenciado. Os agentes dos hosts gerenciados fazem o seguinte:

- Reúnem informações sobre a SAN, consultando comutadores e dispositivos para obtenção de informações sobre o atributo e a topologia.

© Copyright IBM Corp. 2002, 2003

ROS nº 03/2005 - CN
GPMI - CORREIOS
Fls. Nº 1504
3698
Doc.

- Reúnem informações ao nível do host, como sistemas de arquivos e mapeamento para LUNs (Unidades lógicas).
- Reúnem informações sobre o evento e outras informações detectadas pelos HBAs (Adaptadores de Barramento do Host).

Gerenciamento da Rede da Área de Armazenamento

O gerenciamento da SAN descobre automaticamente os componentes e dispositivos da SAN, além da topologia do ambiente de rede de área de armazenamento. É possível monitorar a utilização do armazenamento na SAN e determinar a disponibilidade dos componentes da SAN.

Descoberta

O processo de localização de recursos dentro de uma empresa, incluindo a detecção da topologia da rede, é chamada de *descoberta*. Os dados coletados são armazenados no banco de dados do Tivoli Storage Area Network Manager. O Tivoli Storage Area Network Manager utiliza os dois métodos a seguir para descobrir sua rede:

Na banda
O agente em cada host gerenciado coleta informações sobre o próprio sistema host, incluindo informações sobre sistema de arquivos. Os comandos são enviados por meio das placas HBA que conectam o sistema host à SAN para reunir informações sobre os dispositivos.

Fora da banda
O gerenciador também pode utilizar consultas do SNMP para descobrir informações sobre comutadores da estrutura selecionados. As informações sobre MIB (Management Information Base) são coletadas a partir desses comutadores.

Uma descoberta é acionada por estes eventos:

- Um usuário solicita uma descoberta (executar poll agora).
- Ocorre um evento que faz com que o IBM Tivoli Storage Area Network Manager execute uma descoberta.
- Uma descoberta planejada ou periódica é iniciada. Uma descoberta planejada se torna padrão a cada 24 horas.
- Um host gerenciado ou um agente SNMP foi incluído.

A Tabela 1 explica quando é executada uma descoberta completa e uma descoberta de topologia.

Tabela 1.

Tipos de Descoberta	Uma Descoberta É Executada Quando:
Completa Dependendo do número de objetos a descobrir, uma descoberta completa pode levar muito tempo para concluir. É possível especificar quando executar uma descoberta completa.	• Um usuário pede uma descoberta (poll agora) • Uma descoberta planejada ou periódica é iniciada • Um host gerenciado é adicionado

10289
A

Tabela 1. (continuação)

Tipos de Descoberta	Uma Descoberta É Executada Quando:
Topologia Este tipo de descoberta leva menos tempo para executar do que uma descoberta completa. Entretanto, uma descoberta de topologia não atualiza as exibições centradas no host ou no dispositivo. Essas exibições são atualizadas quando uma descoberta completa for executada.	• Quando o IBM Tivoli Storage Area Network Manager é iniciado • Quando o IBM Tivoli Storage Area Network Manager detecta alterações na SAN • Quando um agente SNMP (chave) é adicionado

Os dados coletados de hosts gerenciados são armazenados no banco de dados DB2.

A coleta de dados é executada por planejamento e por eventos. Um planejamento aciona a descoberta e a torna padrão a cada 24 horas. Quando o Tivoli Storage Area Network Manager detecta um evento em um comutador da estrutura, uma nova descoberta começa.

Descoberta Completa

Como uma descoberta completa pode demorar muito, dependendo do número de objetos que IBM Tivoli Storage Area Network Manager tem que descobrir, você pode selecionar estas opções:

- Nunca executar a descoberta completa (somente descoberta de topologia).
- Somente executar a descoberta completa quando o usuário selecionar **Poll Agora**.
- Somente executar a descoberta completa durante uma descoberta periódica ou planejada.
- Executar a descoberta completa quando o usuário selecionar **Poll Agora** ou durante uma descoberta periódica ou planejada.

Você pode selecionar essas opções utilizando o comando **srmcp ConfigService set**. Consulte *IBM Tivoli Storage Area Network Manager: Guia do Usuário*.

Os valores padrão são definidos da seguinte forma:

- IBM Tivoli Bonus Pack para SAN Management – nunca executa uma descoberta completa.
- IBM Tivoli Storage Area Network Manager – executa uma descoberta completa quando o usuário seleciona **Poll Agora** e quando uma descoberta periódica ou planejada é iniciada.

Quando você escolhe nunca executar uma descoberta completa (somente descoberta de topologia), somente as informações do nível mais superior serão apresentadas nas exibições centradas no dispositivo e no host. Quando você altera o valor da propriedade **FullAttributeScan** de **Nunca** para outra definição de atributo, os dados que estão atualmente no banco de dados aparecem nas exibições centradas nos dispositivos e no host. Nesse ponto, os dados no banco de dados podem ser dados antigos e podem não representar a exibição lógica real. As informações do banco de dados são atualizadas depois que a próxima descoberta completa for executada.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1505
3698
Doc.

Descoberta de SCSI na Internet

O Tivoli Storage Area Network Manager também suporta a descoberta de iSCSI (Internet SCSI). A descoberta de iSCSI é executada independentemente da descoberta feita pelo Tivoli Storage Area Network Manager e exige que você ative a descoberta de IP do Tivoli NetView. Para obter informações adicionais, consulte "Suporte à Internet SCSI" na página 5.

Exibições da Topologia

O Tivoli Storage Area Network Manager extrai informações sobre estrutura a partir do banco de dados e utiliza o Tivoli NetView para exibir a topologia da estrutura. A Tabela 2 descreve as exibições disponíveis para as SANs. Para cada dispositivo descoberto e exibido, é possível abrir um diálogo de propriedades que mostra os atributos e as conexões associados a esse dispositivo.

Tabela 2. Descrição das Exibições da SAN a partir do Tivoli NetView

Exibições da SAN	Descrição
Símbolos da SAN (do Submapa Raiz)	Exibe um símbolo para cada SAN. Dê um clique duplo em um símbolo da SAN para exibir o seu submapa. A partir de um submapa você pode optar por uma das seguintes exibições: • Exibição de Topologia: Exibe a SAN inteira com dois tipos de símbolos, um para os elementos da conexão da SAN e outro para cada segmento da estrutura. • Exibição em Zonas: Exibe a SAN como um agrupamento de zonas.
Centrada no host	Exibe todos os sistemas host e suas relações lógicas com dispositivos locais e conectados à SAN. Não exibe os comutadores e outros dispositivos de conexão.
Centrada no dispositivo	Exibe todos os dispositivos de armazenamento e suas relações lógicas com todos os hosts. Não exibe os comutadores e outros dispositivos de conexão.

Eventos do SNMP

O IBM Tivoli Storage Area Network Manager pode enviar eventos, que representam uma alteração no estado da estrutura, para qualquer console do evento dentro da empresa do qual o IBM Tivoli Storage Area Network Manager participa. Esses eventos são gerados nos formatos SNMP e Tivoli Enterprise Console.

Detecção de Erros e Isolamento de Falhas

A função EDFI (Detecção de Erros e Isolamento de Falhas) ajuda na determinação de problemas em links de interconexão SAN Fibre Channel. A EDFI identifica o hardware com defeito utilizando uma técnica de análise de falhas previstas com base na modelagem estatística das distribuições da falha do componente. A EDFI procura os dados de erros temporários pela SAN e analisa-os quanto a padrões. O hardware ótico e elétrico muitas vezes falha de forma tal que condições intermitentes podem ser identificadas antes que se tornem uma falha permanente. Além disso, o isolamento de falhas é feito para isolar o componente avariado. O objetivo é identificar a ótica com falha e os componentes de interconexão e notificar os usuários antes que realmente ocorra uma falha de hardware. É importante que essa notificação seja resolvida rapidamente. O componente com as taxas de erros temporários elevadas deve ser substituído antes que se torne realmente uma falha permanente. A EDFI não analisa erros para componentes

internos tais como fontes de alimentação. Sua função é analisar contadores associados à transmissão de dados em links SAN. A EDFI reúne contadores de erros temporários para a SAN inteira e analisa a freqüência e a localização dos erros utilizando os métodos estatísticos.

O segredo de utilizar a EDFI com êxito é identificar e remover o componente apropriado antes que ele falhe permanentemente. Alguns motivos para remover um componente antes que ele realmente falhe são os seguintes:

- Uma taxa alta de erros temporários causa problemas de desempenho. Em alguns casos, eles podem ser muito graves.
- Aguardar por uma falha de hardware significa a substituição não planejada do equipamento quando a falha realmente ocorrer. Com a EDFI, a substituição do equipamento pode ser planejada e executada de uma forma menos atrapalhada para os aplicativos que processam dados no link afetado.
- Algumas falhas (cabos quebrados são um ótimo exemplo) podem nunca aparentar um erro permanente. Esta condição deixa o sistema com um link defeituoso indefinidamente.
- Sistemas hosts, sistemas de armazenamento e procedimentos de recuperação de erro de componentes da SAN em resposta a erros repetitivos intermitentes podem causar alterações imprevisíveis na configuração de E/S do sistema, da SAN Fibre Channel ou de ambas. Isso pode afetar a disponibilidade do sistema e do armazenamento.

O Tivoli Storage Area Network Manager fornece uma interface com o usuário EDFI a partir do console do Tivoli NetView que permite gerenciar notificações EDFI e conjuntos de regras. A EDFI gera eventos padrões do Tivoli Enterprise Console que podem ser utilizados para fins de relatório. A EDFI pode detectar os componentes de hardware com falha antes que se tornem falhas de hardware permanente. A EDFI relata componentes com falha no log de Propriedades de EDFI e como um símbolo EDFI no próprio dispositivo na interface de topologia do gerenciador de SAN.

Os conjuntos de regras contêm limites e critérios específicos utilizados pela análise de falhas previstas e funções associadas ao isolamento de falhas do IBM Tivoli Storage Area Network Manager. Os produtos de hardware são alterados com freqüência e os conjuntos de regras permitem que o IBM Tivoli Storage Area Network Manager se atualize com todas as alterações necessárias para executar as operações da EDFI. Os conjuntos de regras podem ser copiados no diretório apropriado e exibidos pelo IBM Tivoli Storage Area Network Manager dinamicamente. Para obter informações adicionais sobre a EDFI, consulte "Configurando o IBM Tivoli Storage Area Network Manager para EDFI" na página 123.

Suporte à Internet SCSI

O Tivoli Storage Area Network Manager fornece suporte básico para descoberta e monitoração de dispositivos iSCSI através do Tivoli NetView. O iSCSI é um padrão de mercado que permite que protocolos de E/S em bloco SCSI (comandos, seqüências e atributos) sejam enviados por uma rede usando o protocolo TCP/IP.

A arquitetura SCSI é baseada em um modelo de cliente/servidor. A Internet SCSI leva esse modelo em conta ao fornecer pedidos de armazenamento por redes TCP/IP. O (*iniciador*) do cliente, em geral, é um sistema host tal como um servidor de arquivos que emite pedidos de leitura ou gravação. O (*destino*) do servidor é um recurso tal como uma matriz de discos que responde a pedidos do cliente. O

1028
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1506
3698
Doc.

cliente é o iniciador e emite os comandos. O servidor é um destino que preenche os pedidos. Os iniciadores e os destinos são identificados pelos nomes iSCSI WWU (world wide unique).

O protocolo iSNS é um protocolo de gerenciamento da memória IETF (Internet Engineering Task Force) complementar para o gerenciamento de dispositivos iSCSI. Esse protocolo permite que dispositivos e hosts de armazenamento registrem-se com um servidor iSNS. Subseqüentemente, os hosts podem consultar o servidor iSNS ou receber atualizações assíncronas do servidor iSNS sobre o status dos dispositivos de armazenamento.

O protocolo iSNS permite que as funções do servidor iSNS sejam implementadas em vários dispositivos, tais como: chaves, roteadores, controladores de armazenamento e nós de console de gerenciamento. O suporte iSCSI do IBM Tivoli Storage Area Network Manager pode ser utilizado independentemente ou em conjunto com a estrutura de gerenciamento iSNS. Quando o iSNS é utilizado em conjunto com o IBM Tivoli Storage Area Network Manager, o carregamento dos arquivos iSNS permitem que você utilize o navegador da MIB no Tivoli NetView. Você pode utilizar o navegador da MIB para consultar o servidor iSNS e exibir o status dos dispositivos iSCSI. Para obter informações adicionais sobre iSCSI ou iSNS, consulte o seguinte Web site:

```
http://www.ietf.org
```

10285
A.

O IBM Tivoli Storage Area Network Manager fornece este suporte:

- Todos os dispositivos iSCSI descobertos na rede IP podem ser colocados em um SmartSet iSCSI exclusivo. O usuário também pode criar SmartSets separados para dispositivos do iniciador e dispositivos de destino iSCSI.
- O utilitário que suporta a descoberta iSCSI chama-se programa **nvsniffer**. O programa **nvsniffer** é fornecido pelo Tivoli NetView. O programa **nvsniffer** utiliza um arquivo de configuração para:
  - Controlar quais serviços descobrirá.
  - Determinar qual serviço o SmartSets criará.
  - Determinar quais portas testará para um determinado serviço.
  - Determinar se utilizará os testes personalizados para descobrir e verificar o status de um serviço.
- As MIBs iSCSI e iSNS (Internet Storage Name Service) estão localizadas em um diretório. Você pode carregá-las no NetView por meio da função de carregamento MIB do NetView.
- Os arquivos de definição de traps MIB iSCSI são utilizados pelo processamento de eventos do Tivoli NetView (filtragem de eventos, encaminhamento, pager, e–mail e ações personalizadas).

Descoberta iSCSI

A descoberta iSCSI é executada independentemente da descoberta feita pelo IBM Tivoli Storage Area Network Manager. A descoberta iSCSI é feita pelo programa **nvsniffer** e pode ser planejada para atualizar os SmartSets iSCSI em intervalos específicos. Se você executar **nvsniffer** regularmente, o programa avisará quando um serviço foi desativado por sete dias consecutivos e excluirá automaticamente o objeto do serviço.

É possível iniciar a descoberta iSCSI por meio do menu do Tivoli NetView. Você também pode iniciar ou parar a descoberta iSCSI pela interface da linha de comandos. Você pode personalizar o planejamento para a descoberta iSCSI utilizando o comando **nvsniffer** do Tivoli NetView. Para obter informações sobre o comando **nvsniffer**, consulte *IBM Tivoli Storage Area Network Manager: Guia do Usuário.*

O IBM Tivoli Storage Area Network Manager fornece suporte básico para descoberta e monitoração de dispositivos iSCSI através do Tivoli NetView. O IBM Tivoli Storage Area Network Manager requer o seguinte para a descoberta de iSCSI:

- O dispositivo deve ter o suporte MIB iSCSI e SNMP.
- O dispositivo deve ser configurado de modo que o suporte a iSCSI MIB esteja ativado. Alguns dispositivos não ativam automaticamente o suporte iSCSI (por exemplo, os roteadores do comutador iSCSI). A configuração pode ser feita pela interface de gerenciamento da configuração do dispositivo.
- O dispositivo iSCSI deve ser descoberto primeiro como um dispositivo IP antes que **nvsniffer** possa descobri-lo como um dispositivo iSCSI.

A descoberta de dispositivo iSCSI exige que se ative a descoberta IP do Tivoli NetView. O Tivoli NetView fornecido com o IBM Tivoli Storage Area Network Manager tem a descoberta IP desativada. Para obter informações sobre como ativar a descoberta IP e iniciar a descoberta do dispositivo iSCSI, consulte "Configurando o IBM Tivoli Storage Area Network Manager para a Descoberta de iSCSI" na página 118.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1577
3698
Doc.

Interfaces para o Tivoli Storage Area Network Manager

Esta seção descreve o tipo de interfaces disponíveis no Tivoli Storage Area Network Manager.

- Console do IBM Tivoli Storage Area Network Manager

  O IBM Tivoli Storage Area Network Manager utiliza o Tivoli NetView para exibir a topologia da estrutura e eventos no banco de dados de eventos.

- Interface da linha de comando

  É possível utilizar a interface da linha de comandos para emitir comando de log, comandos de serviço do gerenciador ou quando se criam scripts que submetem comandos. Consulte o *IBM Tivoli Storage Area Network Manager: Guia do Usuário* para obter mais informações sobre comandos de registro e serviço do gerenciador.

Integrando o IBM Tivoli Storage Area Network Manager à Solução de Gerenciamento SNMP

O Tivoli Storage Area Network Manager foi desenvolvido para fazer parte de uma solução de gerenciamento SNMP integrada. Se você já estiver implementando uma solução SNMP para a sua rede de armazenamento, o Tivoli Storage Area Network Manager integrará e incluirá valor a essa solução. Se você ainda não estabeleceu uma solução SNMP, o Tivoli NetView pode servir como o seu console de gerenciamento SNMP.

Para obter mais informações sobre configuração, consulte o Capítulo 9, "Configurando o IBM Tivoli Storage Area Network Manager", na página 107.

1028
A

Capítulo 2. Planejando a Instalação

Importante

Antes de instalar o IBM Tivoli Storage Area Network Manager, certifique-se de que a SAN esteja operacional. O IBM Tivoli Storage Area Network Manager não pode ser executado em uma SAN não operacional. Verifique o seguinte:

- Você deve ter instalado as placas HBA (adaptador de barramento de host) apropriadas e drivers de dispositivo (por exemplo, o HBA QLogic e drivers de dispositivo). Para EDFI, a API HBA comum da fase 2 deve ser instalada no host gerenciado. Isto é obrigatório para reunir estatísticas de portas. Para obter uma lista de compatibilidade de dispositivos, consulte o seguinte endereço da Web:

  `http://www-3.ibm.com/software/sysmgmt/products/support/`

  Selecione IBM Tivoli Storage Area Network Manager na lista drop down.
- Certifique-se de que o pacote de drivers de dispositivo para o HBA possua suporte instalado para a API HBA comum. Se esse pacote não possuir suporte para a API HBA comum, certifique-se de ter executado um programa de instalação separado para ele. Em caso de dúvidas, entre em contato com o fabricante do HBA.
- O IBM Tivoli Storage Area Network Manager (componente gerenciador e consoles remotos) e todos os hosts gerenciados devem ter nomes de host completos. O componente gerenciador deve ter um endereço IP estático.
- A rede deve utilizar o DNS.
- É altamente recomendável que a EDFI seja desativada durante a instalação e a reconfiguração de hardware da SAN. Isto evitará que apareçam eventos falsos de erros nos logs de propriedades da EDFI assim como nos ícones do NetView.

Nota:

- O IBM Tivoli Storage Area Network Manager somente oferece suporte para IDs de usuário definidos localmente no computador. Isso inclui os IDs de usuário para o DB2, o Tivoli NetView e o gerenciador.
- Antes de instalar o IBM Tivoli Storage Area Network Manager, consulte este Web site para quaisquer documentos em *Flash*:

  `http://www-3.ibm.com/software/sysmgmt/products/support/`

  Selecione IBM Tivoli Storage Area Network Manager na lista drop-down de produto.
- Existem dois CDs do produto:
  - Primeiro CD – contém o gerenciador e o console remoto
  - Segundo CD – contém os agentes
- Antes de instalar o IBM Tivoli Storage Area Network Manager, consulte os arquivos LEIA-ME no CD do produto. Os arquivos LEIA-ME estão no diretório readme. Os arquivos são:

  `readme_`*`language`*`.txt`

© Copyright IBM Corp. 2002, 2003

ROS nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 1508
Doc. 3698

Onde *idioma* pode ser uma das opções a seguir:
- en – Inglês
- de – Alemão
- es – Espanhol
- fr – Francês
- it – Italiano
- ja – Japonês
- ko – Coreano
- pt_BR – Português do Brasil
- zh_CN – Chinês Simplificado
- zh_TW – Chinês Tradicional

Requisitos do Sistema para o Tivoli Storage Area Network Manager

Esta seção fornece informações sobre os requisitos de hardware e software para o Tivoli Storage Area Network Manager.

Requisitos de Armazenamento

Os requisitos de armazenamento para o IBM Tivoli Storage Area Network Manager são os seguintes:

Tabela 3. Requisitos de Armazenamento para o IBM Tivoli Storage Area Network Manager

Componente	Espaço em Disco	RAM	Memória Virtual
Gerenciador (Windows 2000)	1 GB, espaço temporário em disco de 350 MB para instalar (isso inclui o Tivoli NetView)	1 GB	2 GB
Gerenciador (AIX)	200 MB em um diretório temporário, 200 MB no diretório de instalação e 30 MB no diretório inicial (/home)	1 GB	2 GB
Agente	200 MB, o agente também requer um espaço em disco temporário de 100 MB para instalação	256 MB	512 MB
Console remoto do IBM Tivoli Storage Area Network Manager	1024 MB	512 MB	1024 MB

O armazenamento mínimo requerido para a instalação do produto de pré-requisito é o seguinte:

Tabela 4. Espaço em Disco Requerido para a Instalação de Produtos de Pré-requisito

Produto	Espaço em Disco
DB2	400 MB

Requisitos do Gerenciador (Windows 2000)

Os requisitos do Windows 2000 incluem:

- Uma máquina dedicada (DB2 e gerenciador na mesma máquina e que execute apenas o IBM Tivoli Storage Area Network Manager).
- Máquina: Processador Pentium III de 1 GHz (mínimo).
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema Operacional: Sistema operacional Microsoft Windows 2000 Server, Advanced Server ou Professional com Service Pack 3. Também é necessário ter o serviço SNMP instalado e certificar-se de que o nome da comunidade SNMP seja **público**.
- Servidor DB2 (Database 2) UDB (Universal Database) Enterprise Edition Versão 7.2 com FixPak 8 instalado. Os CDs do DB2 são fornecidos com o IBM Tivoli Storage Area Network Manager. O DB2 deve ser instalado no gerenciador *antes* da instalação do IBM Tivoli Storage Area Network Manager.
- Tivoli NetView versão 7.1.3 (instalado com o IBM Tivoli Storage Area Network Manager). Se você tiver uma versão do Tivoli NetView anterior à versão 7.1.1, será necessário remover manualmente a instalação dessa versão antes de instalar o IBM Tivoli Storage Area Network Manager.

  Nota: O IBM Tivoli Storage Area Network Manager *não* oferece suporte para o console da Web Tivoli NetView.
- É necessária a utilização de um sistema de arquivos NTFS para o diretório de instalação.
- A resolução de vídeo deve ser 1024x768 com 256 cores.

Requisitos do Gerenciador (AIX)

Os requisitos do gerenciador do AIX incluem:

- Uma máquina dedicada (DB2 e gerenciador na mesma máquina e que execute apenas o IBM Tivoli Storage Area Network Manager).
- Máquina: AIX RS/6000 de 375 MHz (mínimo).
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema Operacional: AIX versão 5.1 que seja executado em sistemas de 32 ou 64 bits. Você também deve ter as correções do sistema operacional para suporte ao JRE 1.3.1.

  Se estiver executando o AIX 5.1, o Java 1.3.1 exigirá o Nível de Manutenção Recomendado 02 do AIX 5100. Faça o download deste pacote no seguinte Web site:

  `http://techsupport.services.ibm.com/rs6000/fixes/`

  Se estiver utilizando o AIX 5.1 com Nível de Manutenção 2, deverá aplicar uma correção para o defeito 379463 do AIX. O número de APAR é IY34030. Faça o download desta correção no seguinte Web site:

  `https://techsupport.services.ibm.com/server/aix.fdc`

  Em Search by, digite **APAR number**. Na cadeia Search, digite **IY34030**.
- Servidor DB2 (Database 2) UDB (Universal Database) Enterprise Edition Versão 7.2 com FixPak 8 instalado. Os CDs do DB2 são fornecidos com o IBM Tivoli Storage Area Network Manager. O DB2 deve ser instalado no gerenciador *antes* da instalação do IBM Tivoli Storage Area Network Manager.

O Tivoli NetView não está instalado ou não é suportado no gerenciador do AIX. O console remoto tem suporte no Windows 2000 e no XP.

10281 A
POSTO DE ATENDIMENTO CN CPMI CORREIOS 1569 Doc. 3698

Requisitos do Console Remoto do IBM Tivoli Storage Area Network Manager

O console remoto requer o seguinte:

- Máquina: Processador Pentium III de 450 MHz.
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema operacional:
  - Windows 2000: Professional, Server ou Advanced Server. Cada um deve ter o Service Pack 3 instalado.
  - Windows XP.
- O serviço SNMP precisa estar instalado e o nome da comunidade SNMP deve estar definido como **Público**.
- Deve ser utilizado um sistema de arquivos NTFS para o diretório de instalação.
- A resolução de vídeo deve ser de 1024x768 com 256 cores.

O console remoto do IBM Tivoli Storage Area Network Manager não pode ser instalado no servidor gerenciador (o console é instalado com o gerenciador). Entretanto, pode ser instalado em um host gerenciado.

Requisitos do Agente

Esta seção fornece informações sobre os requisitos para os agentes em sistemas operacionais diferentes.

Agente do Windows

Os requisitos para o agente do Windows incluem:

- Máquina: Processador Pentium III de 400 MHz.
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema operacional – um dos seguintes:
  - Windows NT 4.0 (com Service Pack 6A)
  - Windows 2000: Professional, Server ou Advanced Server (cada um com o Service Pack 3)
- Nível e HBA apropriados. Consulte o seguinte URL:

  `http://www-3.ibm.com/software/sysmgmt/products/support/`

  Selecione IBM Tivoli Storage Area Network Manager na lista drop down.

Agente do AIX

Os requisitos para o agente do AIX incluem:

- Máquina: Processador 43P–150 de 375 MHz no mínimo.
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema Operacional: AIX 5.1 ou 5.2. Você também deve ter as correções do sistema operacional para suporte ao JRE 1.3.1.

  Se estiver executando o AIX 5.1, o Java 1.3.1 exigirá o Nível de Manutenção Recomendado 02 do AIX 5100. Você pode fazer download deste pacote em:

  `http://techsupport.services.ibm.com/rs6000/fixes/`

  Se estiver utilizando o AIX 5.1 com Nível de Manutenção 2, deverá aplicar uma correção para o defeito 379463 do AIX. O número de APAR é IY34030. Faça o download desta correção no seguinte Web site:

10279
A

https://techsupport.services.ibm.com/server/aix.fdc

Em Search by, digite **APAR number**. Na cadeia Search, digite **IY34030**.

- Nível e HBA apropriados. Consulte o seguinte URL:
  http://www-3.ibm.com/software/sysmgmt/products/support/

  Selecione IBM Tivoli Storage Area Network Manager na lista drop down.

Agente do Solaris

Os requisitos para o agente do Solaris incluem:

- Máquina: Processador Ultra 5S de 360 MHz no mínimo.
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema Operacional: Ambiente Operacional Solaris 2.6 ou 2.8. Esse ambiente operacional é denominado Solaris. Deve possuir correções de sistema operacional para oferecer suporte ao JRE 1.3.1.

  Para obter informações sobre as correções do sistema operacional, consulte:
  http://java.sun.com/j2se/1.3/install-solaris-patches.html
- Nível e HBA apropriados. Consulte o seguinte URL:
  http://www-3.ibm.com/software/sysmgmt/products/support/

  Selecione IBM Tivoli Storage Area Network Manager na lista drop–down de produto.

Agente do Linux

Os requisitos para o agente do Linux incluem:

- Máquina: Processador Pentium III com um processador de 400 MHz.
- Requisitos de memória e espaço em disco: consulte "Requisitos de Armazenamento" na página 10.
- Sistema operacional, um dos seguintes:
  - Linux Redhat Advanced Server versão 2.1 (32 bits) com kernel 2.4.9.
  - SuSE Linux Enterprise Server versão 7.0 (32 bits) com kernel 2.4.7.
- Nível e HBA apropriados. Consulte o seguinte URL:
  http://www-3.ibm.com/software/sysmgmt/products/support/

  Selecione IBM Tivoli Storage Area Network Manager na lista drop–down de produto.

Considerações sobre Compatibilidade

Se você possui um agente do IBM Tivoli Storage Area Network Manager AIX 4.3.3 em um host gerenciado, esse agente poderá coexistir com um gerenciador do release 2.

Limitações

O scanner do evento não é mais executado no QLogic QLA2200 HBA. Isto significa que o agente não notificará o gerenciador de eventos reunido dentro da faixa para essa malha. Em vez disso, as chaves podem ser configuradas para enviar eventos fora da faixa ao gerenciado da malha.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1510
Nº Doc. 3698

Outros Suportes

O IBM Tivoli Storage Area Network Manager instala e utiliza automaticamente os componentes listados.

- O Tivoli NetView (automaticamente instalado com o gerenciador e o console remoto do Windows)
- IBM JRE 1.3.1 (instalado automaticamente com o gerenciador, os hosts gerenciados e o console remoto). Esse JRE não é utilizado como o padrão do sistema; somente é utilizado para o IBM Tivoli Storage Area Network Manager.

Se você planeja enviar eventos do IBM Tivoli Storage Area Network Manager para um receptor, deve possuir suporte de programação para pelo menos um dos itens a seguir:

- SNMP
- O Tivoli Enterprise Console

Ambiente da SAN

Os hosts gerenciados devem compartilhar uma conexão de rede de área de armazenamento comum com dispositivos de armazenamento compartilhado. Um HBA (adaptador de barramento de host) da SAN e os drivers de dispositivo apropriados da SAN também são necessários em cada host gerenciado. Nem todos os hosts gerenciados e dispositivos devem estar conectados a uma única SAN em comum. Ou seja, um conjunto de hosts gerenciados e dispositivos pode estar conectado a uma SAN, enquanto um conjunto separado pode estar conectado a uma segunda SAN. O Tivoli Storage Area Network Manager pode monitorar essas duas SANs.

Para obter informações sobre o ambiente da SAN e os dispositivos suportados, consulte o seguinte Web site:

`http://www-3.ibm.com/software/sysmgmt/products/support/`

Selecione IBM Tivoli Storage Area Network Manager na lista drop–down de produto.

Visão Geral das Etapas de Instalação para Instalar o IBM Tivoli Storage Area Network Manager

Você instalará esses componentes para o IBM Tivoli Storage Area Network Manager. Consulte Tabela 5.

Tabela 5. Componentes do Tivoli Storage Area Network Manager

Componente	Descrição	Local de Instalação
Gerenciador (Windows 2000)	Componente gerenciador do Tivoli Storage Area Network Manager. Esse componente inclui o Tivoli NetView e o console do IBM Tivoli Storage Area Network Manager.	Computador do gerenciador dedicado.
Gerenciador (AIX)	Componente gerenciador do Tivoli Storage Area Network Manager.	Computador do gerenciador dedicado.

10277
A.

Tabela 5. Componentes do Tivoli Storage Area Network Manager (continuação)

Componente	Descrição	Local de Instalação
Agente	O agente desempenha o processo de descoberta em banda em um host conectado à SAN.	Esse componente pode ser instalado no computador do gerenciador ou em um computador diferente.
Console remoto do IBM Tivoli Storage Area Network Manager	Opcional e instalado em um computador diferente do gerenciador. Esse programa de instalação não pode ser instalado no mesmo computador do gerenciador. Se você tiver instalado o console remoto do IBM Tivoli Storage Area Network Manager em um computador, não poderá instalar o gerenciador nesse computador.	Um computador diferente do gerenciador.

AOS nº 03/2005 - CN
CPMI - CORREIOS
Nº 1511
Doc 3698

Etapas de Instalação para um Gerenciador do Windows

As etapas básicas de instalação de um gerenciador do Windows são as seguintes:

1. Siga as etapas no Capítulo 3, "Preparando-se para a Instalação (Gerenciador do Windows)", na página 19. Essa seção fornece informações necessárias para o IBM Tivoli Storage Area Network Manager. Se o DB2 versão 7.2 não estiver instalado com o FixPak 8, essa seção fornecerá informações sobre como instalar o DB2. Ela também fornece informações sobre como instalar o serviço SNMP.
2. Siga as etapas no Capítulo 5, "Instalando o Gerenciador do Windows", na página 59. Essa seção fornece informações sobre como instalar o IBM Tivoli Storage Area Network Manager no computador do gerenciador.
3. Siga as etapas no Capítulo 7, "Instalando o Agente no Host Gerenciado", na página 83. Essa seção fornece informações sobre como instalar o agente no host gerenciado. Se você quiser instalar o agente em computadores diferentes, deverá executar o programa de instalação em cada computador.
4. Esta etapa será opcional se você quiser instalar um console remoto do IBM Tivoli Storage Area Network Manager. Siga as etapas no Capítulo 8, "Instalando o Console Remoto do IBM Tivoli Storage Area Network Manager", na página 95. Se você quiser instalar o console remoto do IBM Tivoli Storage Area Network Manager em computadores diferentes, deverá executar o programa de instalação em cada computador.
5. Configure o IBM Tivoli Storage Area Network Manager. Consulte Capítulo 9, "Configurando o IBM Tivoli Storage Area Network Manager", na página 107.
6. Instale o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager. Essa etapa é opcional. Consulte Capítulo 11, "Instalando o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager", na página 153.

Se você quiser remover a instalação do IBM Tivoli Storage Area Network Manager, consulte o Capítulo 12, "Removendo a Instalação do IBM Tivoli Storage Area Network Manager", na página 171.

Etapas de Instalação para um Gerenciador do AIX

As etapas básicas de instalação de um gerenciador do AIX são as seguintes:

1. Siga as etapas no Capítulo 4, "Preparando-se para a Instalação (Gerenciador do AIX)", na página 35. Essa seção fornece informações necessárias para o IBM Tivoli Storage Area Network Manager. Se o DB2 versão 7.2 não estiver instalado com o FixPak 8, essa seção fornecerá informações sobre como instalar o DB2.
2. Siga as etapas no Capítulo 6, "Instalando o Gerenciador do AIX", na página 79. Essa seção fornece informações sobre como instalar o IBM Tivoli Storage Area Network Manager no computador do gerenciador.
3. Siga as etapas no Capítulo 7, "Instalando o Agente no Host Gerenciado", na página 83. Essa seção fornece informações sobre como instalar o agente no host gerenciado. Se você quiser instalar o agente em computadores diferentes, deverá executar o programa de instalação em cada computador.
4. Instale um console remoto do IBM Tivoli Storage Area Network Manager. Siga as etapas no Capítulo 8, "Instalando o Console Remoto do IBM Tivoli Storage Area Network Manager", na página 95. Se você quiser instalar o console remoto do IBM Tivoli Storage Area Network Manager em computadores diferentes, deverá executar o programa de instalação em cada computador.
5. Configure o IBM Tivoli Storage Area Network Manager. Consulte Capítulo 9, "Configurando o IBM Tivoli Storage Area Network Manager", na página 107.

6. Instale o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager. Essa etapa é opcional. Consulte Capítulo 11, "Instalando o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager", na página 153.

Se o IBM Tivoli Storage Area Network Manager versão 1.1 estiver instalado e você deseja fazer upgrade para a versão 1.2, consulte Capítulo 10, "Fazendo Upgrade do IBM Tivoli Storage Area Network Manager", na página 129.

Se você quiser remover a instalação do IBM Tivoli Storage Area Network Manager, consulte o Capítulo 12, "Removendo a Instalação do IBM Tivoli Storage Area Network Manager", na página 171.

Fazendo Upgrade do IBM Tivoli Storage Area Network Manager

Para fazer upgrade do IBM Tivoli Storage Area Network Manager versão 1.1.0 ou 1.1.1 para a versão 1.2, siga as etapas em Capítulo 10, "Fazendo Upgrade do IBM Tivoli Storage Area Network Manager", na página 129.

Alterações para o IBM Tivoli Storage Area Network Manager Versão 1.2

As alterações para o IBM Tivoli Storage Area Network Manager versão 1.2 estão resumidas a seguir:

Gerenciador do AIX

O gerenciador do AIX IBM Tivoli Storage Area Network Manager agora é suportado. Quando instalado o gerenciador do AIX, o Tivoli NetView não será instalado ou suportado no AIX. Se desejar ver a exibição da GUI no IBM Tivoli Storage Area Network Manager, instale o console remoto no Windows 2000 ou Windows XP.

Sistemas Operacionais do Host Gerenciado

Os seguintes sistemas operacionais agora são suportados:

- AIX 5.1 e 5.2
- Solaris Operating Environment 2.6 e 2.8
- Linux Redhat Advanced Server Versão 2.1
- SuSE Linux Enterprise Server Versão 7.0

Um host gerenciado da versão 1.1 ainda será executado com o gerenciador da versão 1.2. Porém, funções novas (como EDFI) não são suportadas no host gerenciado da versão 1.1.

Versão Embutida do IBM WebSphere Application Server – Express

Quando você instala o IBM Tivoli Storage Area Network Manager, você automaticamente instala a versão embutida do WebSphere. Não é necessário instalar o WebSphere separadamente. Observe que você encontrará algumas diferenças administrativas quando instalar a versão embutida do WebSphere. Você não verá mais o WebSphere Administrative Console. Existem vantagens no uso da versão embutida do WebSphere. Isto reduz a utilização da memória, é mais fácil de instalar e de manter.

Detecção de Erros e Isolamento de Falhas

A detecção de erros e isolamento de falhas ajuda o usuário a detectar erros na SAN e determinar onde o componente avariado está localizado. Para obter mais informações, consulte o "Configurando o IBM Tivoli Storage Area Network Manager para EDFI" na página 123.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1512
Doc 3698

É altamente recomendável que a EDFI seja desativada durante a instalação e a reconfiguração de hardware da SAN. Isto evitará que apareçam eventos falsos de erros nos logs de propriedades da EDFI assim como nos ícones do NetView.

iSCSI (Internet SCSI)
Internet SCSI é um padrão proposto pelo mercado que permite que sistemas de computadores centrais executem operações em bloco de entrada/saída de dados com diversos dispositivos. Os dispositivos de destino podem incluir dispositivos de disco e fita e dispositivos de armazenamento. O protocolo Internet SCSI define um meio de transferir comandos e dados SCSI pelas redes TCP/IP. Para obter mais informações sobre iSCSI, consulte "Configurando o IBM Tivoli Storage Area Network Manager para a Descoberta de iSCSI" na página 118.

Tivoli NetView
Feito o upgrade do Tivoli NetView para a versão 7.1.3.

Endereços IP Dinâmicos
Para os hosts gerenciados e os consoles remotos é possível utilizar os endereços IP dinâmicos em vez dos endereços IP estáticos. O gerenciador ainda deve utilizar endereços IP estáticos.

JRE Agora foi feito o upgrade de JRE 1.3.0 para JRE 1.3.1.

MQSeries
O MQSeries foi removido deste release.

Console Remoto
O console remoto do IBM Tivoli Storage Area Network Manager agora é suportado no Windows XP.

Classe de Eventos do Tivoli Enterprise Console
No IBM Tivoli Storage Area Network Manager versão 1.1, havia apenas uma classe de eventos do Tivoli Enterprise Console. Este release fornece várias classes. Consulte "Classes de Eventos e Atributos do Tivoli Enterprise Console" na página 213.

Instalação Silenciosa do IBM Tivoli Storage Area Network Manager
A instalação silenciosa do IBM Tivoli Storage Area Network Manager agora é suportada. Consulte Apêndice A, "Instalação Silenciosa do IBM Tivoli Storage Area Network Manager", na página 189.

Capítulo 3. Preparando-se para a Instalação (Gerenciador do Windows)

Antes de poder instalar o IBM Tivoli Storage Area Network Manager, existem várias etapas a serem concluídas. As seções a seguir descrevem essas etapas.

Etapa 1: Verificar Itens Necessários

O IBM Tivoli Storage Area Network Manager exige programas e serviços específicos para que você possa instalá-lo com êxito. A Tabela 6 fornece uma lista de programas e informações necessários para o IBM Tivoli Storage Area Network Manager (gerenciador). A Tabela 7 na página 20 fornece uma lista de programas e informações necessários para a instalação do console remoto. A Tabela 8 na página 21 fornece uma lista de informações necessárias para a instalação dos hosts gerenciados.

Tabela 6. Programas e Informações Necessários para a Instalação do Gerenciador do Windows

Número do Item	Item	Insira Informações Aqui
1	Endereço IP estático no gerenciador. Para verificar um endereço IP estático, consulte "Verificando um Endereço IP Estático" na página 207.	
2	Nome do host completo do computador do gerenciador. Para verificar um nome de host completo, consulte "Verificando Nomes de Host Completos" na página 204. Nomes de host fazem distinção entre maiúsculas e minúsculas (uma limitação do WebSphere).	
3	ID do administrador e senha DB2	
4	DB2 Versão 7.2 com FixPak 8 instalado. Se esse programa não estiver instalado, consulte a "Etapa 4: Instalar o DB2" na página 22.	
5	Uma faixa de sete números de porta (devem estar em ordem seqüencial). Certifique-se de que nenhum outro aplicativo esteja utilizando esses números de porta. Os números de porta padrão são de 9550 a 9556. Esses números de porta padrão são utilizados da seguinte maneira: **9550+0** Porta HTTP. **9550+1** Reservado. **9550+2** Reservado. **9550+3** Reservado. **9550+4** Porta NVDAEMON. **9550+5** Porta NVREQUESTER. **9550+6** Porta SNMPTrapPort na qual são obtidos eventos encaminhados do Tivoli NetView.	

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 3319
Nº Doc. 3698

Tabela 6. Programas e Informações Necessários para a Instalação do Gerenciador do Windows (continuação)

Número do Item	Item	Insira Informações Aqui
6	Tivoli NetView versão 7.1.3. Se esse programa não estiver instalado, o IBM Tivoli Storage Area Network Manager o instalará automaticamente. Se o Tivoli NetView versão 7.1.3 estiver instalado, será configurado pelo programa de instalação. Se o Tivoli NetView versão 7.1.1 estiver instalado, será feito o upgrade para 7.1.3.	
7	Serviço SNMP. Para instalar o Serviço SNMP, consulte a "Etapa 5: Instale o Serviço SNMP" na página 29.	
8	Serviço de Planejamento (Windows 2000)	

Tabela 7. Programas e Informações Necessários para a Instalação do Console Remoto

Número do Item	Item	Insira Informações Aqui
1	Tivoli NetView versão 7.1.3. Se esse programa não estiver instalado, o IBM Tivoli Storage Area Network Manager o instalará automaticamente. Se o Tivoli NetView versão 7.1.3 estiver instalado, será configurado pelo programa de instalação. Se o Tivoli NetView versão 7.1.1 estiver instalado, será feito o upgrade para 7.1.3.	
2	Serviço SNMP. Para instalar o Serviço SNMP, consulte a "Etapa 5: Instale o Serviço SNMP" na página 29.	
3	Serviço de Planejamento (Windows 2000)	
4	Número da porta e nome do host completo do gerenciador. Para verificar o nome do host completo, consulte "Verificando Nomes de Host Completos" na página 204.	
5	Uma faixa de seis números de porta (devem estar em ordem seqüencial). Certifique-se de que nenhum outro aplicativo esteja utilizando esses números de porta. Os números de porta padrão são de 9560 à 9565. Esses números de porta padrão são utilizados da seguinte maneira: **9560+0** Porta HTTP. **9560+1** Reservado. **9560+2** Porta do Servidor Local do Tomcat. **9560+3** Porta Warp do Tomcat. **9560+4** Porta NVDAEMON. **9560+5** Porta NVREQUESTER.	
6	Senha de autenticação do host	

Tabela 8. Programas e Informações Necessários para a Instalação do Agente no Host Gerenciado

Número do Item	Item	Insira Informações Aqui
1	Número da porta e nome do host completo do gerenciador. Para verificar o nome do host completo, consulte "Verificando Nomes de Host Completos" na página 204.	
2	Uma faixa de quatro números de porta (devem estar em ordem seqüencial). Certifique-se de que nenhum outro aplicativo esteja utilizando esses números de porta. Os números de porta padrão são de 9570 a 9573. Esses números de porta padrão são utilizados da seguinte maneira: **9570+0** Porta HTTP. **9570+1** Reservado. **9570+2** Porta do Servidor Local do Tomcat. **9570+3** Porta Warp do Tomcat.	
3	É necessário ter as correções atuais do sistema operacional para oferecer suporte ao JRE 1.3.1. O JRE 1.3.1 é instalado pelo programa de instalação.	
4	Senha de autenticação do host	

Etapa 2: Verificar o Nome do Computador

O IBM Tivoli Storage Area Network Manager exige nomes de host completos para o gerenciador, os hosts gerenciados e o console remoto. Para verificar o nome do computador no Windows, consulte o procedimento a seguir.

Para verificar se o nome do computador está definido corretamente no Windows, siga estas etapas:

1. No desktop, clique com o botão direito do mouse no ícone **Meu computador**.
2. Clique em **Propriedades**.
3. O painel Propriedades do sistema é exibido.
4. Clique na guia **Identificação de rede**.
5. Clique em **Propriedades**.
6. O painel Alterações de identificação é exibido. Verifique se o nome do computador está inserido corretamente. Esse é o nome com o qual o computador será identificado na rede. Além disso, verifique se o nome completo do computador é um nome de host completo. Por exemplo, user1.sanjose.ibm.com é um nome de host completo.
7. Clique em **Mais**.
8. O painel Sufixo DNS e nome de computador NetBIOS é exibido. Verifique se o campo **Sufixo DNS primário** exibe um nome de domínio.

O nome do host completo deve corresponder ao nome do arquivo HOSTS (incluindo caracteres que fazem distinção entre maiúsculas e minúsculas). Para obter informações sobre o arquivo HOSTS, consulte a "Etapa 3: Alterar o Arquivo HOSTS" na página 22.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1014
Fls. Nº
Doc. 3698

Etapa 3: Alterar o Arquivo HOSTS

Ao instalar o Service Pack 3 para o Windows 2000 nos computadores, siga estas etapas para evitar problemas de endereçamento com o Tivoli Storage Area Network Manager. O problema é causado pelo protocolo de resolução de endereços, que retorna o nome abreviado (nome do host incompleto). É possível evitá-lo alterando as entradas nas tabelas de host correspondentes no servidor DNS e no computador local. O nome do host completo deve estar listado antes do nome abreviado.

Para corrigir esse problema, siga estas etapas:

1. No diretório **%SystemRoot%\system32\drivers\etc**, você localizará o arquivo **HOSTS**.
2. Será necessário editar esse arquivo **HOSTS**. Um exemplo de arquivo **HOSTS** está exibido a seguir.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

192.168.123.146     jason     jason.groupa.mycompany.com
```

3. Insira o nome do host completo como a primeira linha a ser pesquisada na tabela. (As linhas precedidas pelo sinal # são linhas de comentário.) Por exemplo, inclua a linha realçada em negrito no arquivo:

```
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

192.168.123.146     jason.groupa.mycompany.com      jason
192.168.123.146     jason     jason.groupa.mycompany.com
```

Nota: Nomes de host fazem distinção entre maiúsculas e minúsculas. Essa é uma limitação do WebSphere. Verifique o nome do host. Consulte "Etapa 2: Verificar o Nome do Computador" na página 21. Por exemplo, se o computador mostrar o nome como JASON (letras maiúsculas), será necessário inserir JASON no arquivo HOSTS.

Etapa 4: Instalar o DB2

Instale o DB2 Versão 7.2. O IBM Tivoli Storage Area Network Manager cria tabelas do DB2 para seus dados. Instale o DB2 no computador do gerenciador (Windows 2000).

Nota: Convém dedicar o DB2 para o IBM Tivoli Storage Area Network Manager. Fazer com que outros aplicativos utilizem o DB2 pode prejudicar o desempenho.

Se você tiver o DB2 Enterprise Edition Versão 7.2 instalado, poderá omitir este procedimento de instalação e seguir as etapas em "Fazendo o Upgrade do DB2 com o FixPak 8" na página 28. Caso contrário, instale o DB2. Para isso, siga as etapas em "Fazendo o Upgrade do DB2 com o FixPak 8" na página 28.

Para instalar o DB2 na unidade C:, siga estas etapas.

1. Efetue login com um ID de usuário com autoridade de administrador para executar o programa de instalação.
2. Coloque o CD do DB2 na unidade de CD-ROM. Se o autorun do Windows estiver ativado, a instalação do DB2 é iniciada automaticamente. O painel **Welcome** é exibido. Clique em **Install (Instalar)**.

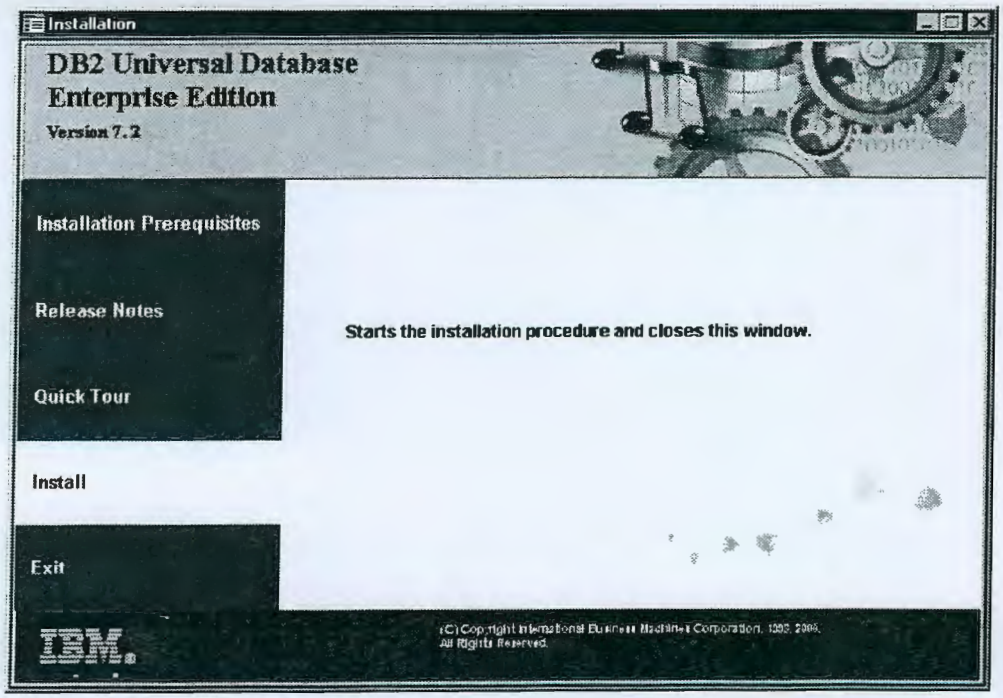


Figura 2. Painel de Instalação do DB2

3. Se o CD não for executado automaticamente, acesse o Windows Explorer e clique na unidade de CD-ROM. À direita da janela do Explorer, dê um clique duplo no programa **setup.exe**.
4. No painel **Select Products**, selecione **DB2 Enterprise Edition**. Clique em **Next** para continuar.

RQS nº 03/2005 - CN
Fls. Nº 3698
Doc.

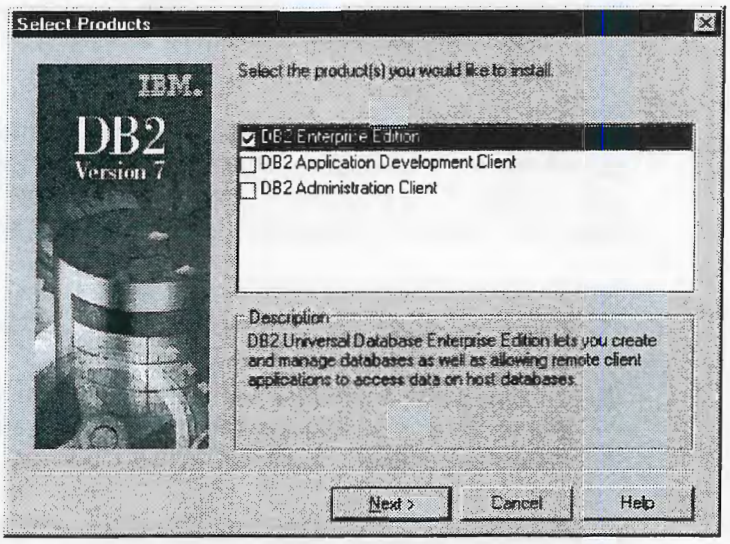


Figura 3. Painel Select Products

1026

5. No painel **Select Installation Type**, selecione uma instalação **Typical**. Clique em **Next** para continuar.

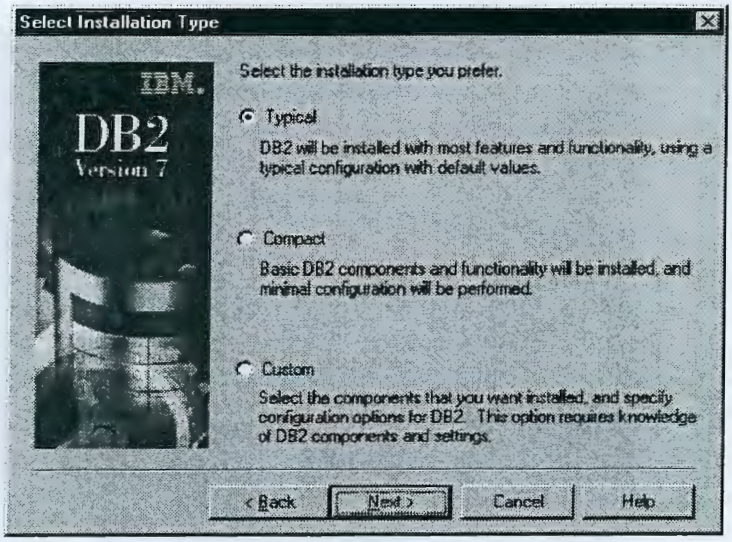


Figura 4. Painel Select Installation Type

6. Se você receber o seguinte painel de informações para o suporte OLE DB, clique em **OK**.

Figura 5. Painel Information

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1516
Nº Doc. 3698

7. No painel **Choose Destination Location**, escolha uma localização para instalar o DB2. O padrão é **C:\Arquivos de programas\SQLLIB**. Clique em **Next** para continuar.

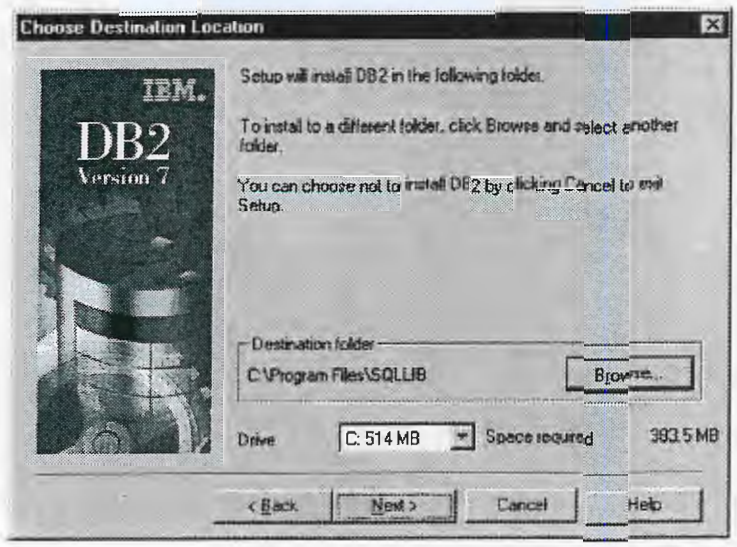


Figura 6. Painel Choose Destination Location

8. No painel **Enter Username and Password for Control Center Server**, insira o nome de usuário e a senha DB2 e clique em **Next**. Se esse nome de usuário ainda não existir, será criado e receberá autoridade administrativa para criar tabelas do DB2 e a permissão **Logon as a service**.

   O ID de usuário DB2 padrão criado é **db2admin**, como uma senha correspondente de **db2admin**. É possível utilizá-lo ou alterá-lo. Os exemplos neste documento utilizam **db2admin** para a instalação do IBM Tivoli Storage Area Network Manager.

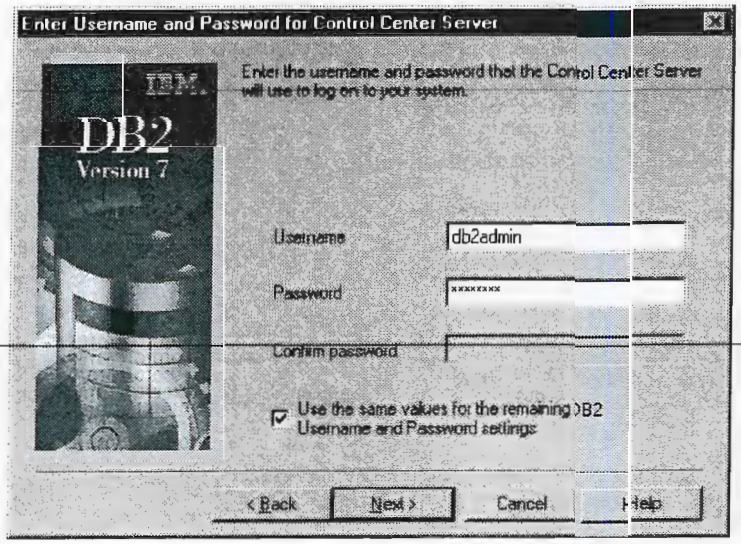


Figura 7. Painel Enter Username and Password for Control Center Server

9. No painel **Start Copying Files**, clique em **Next**.

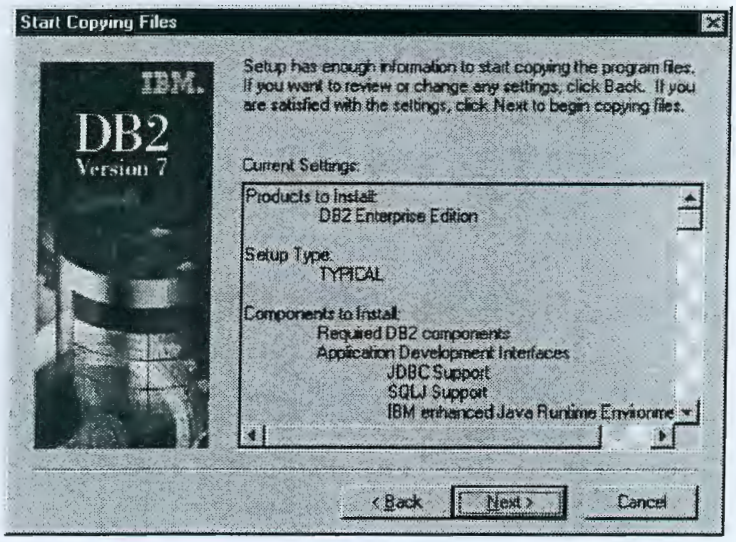


Figura 8. Painel Start Copying Files

O painel **Install OLAP Starter Kit** é exibido. Marque o botão de rádio para **Do not install the OLAP Starter Kit**. Clique em **Continue**. Os componentes do DB2 são instalados.

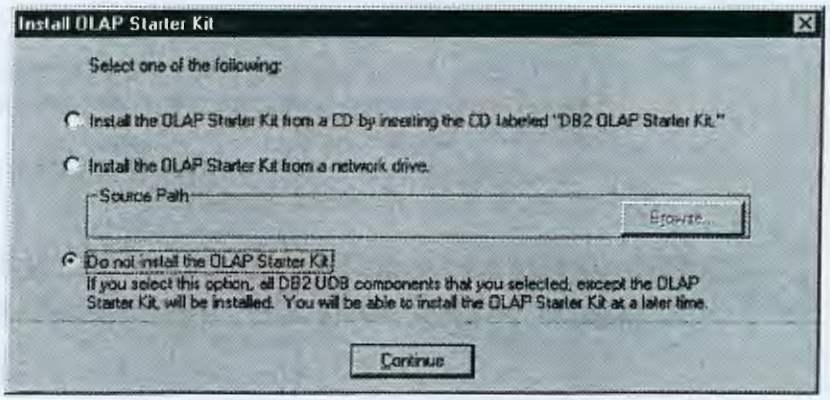


Figura 9. Painel Install OLAP Starter Kit

10265
RQS nº 03/2005 - CN
CPMI - CORREIOS
1517
Fls. Nº
Doc. 3698

10. Clique em **Finish** no painel **Setup Complete**.

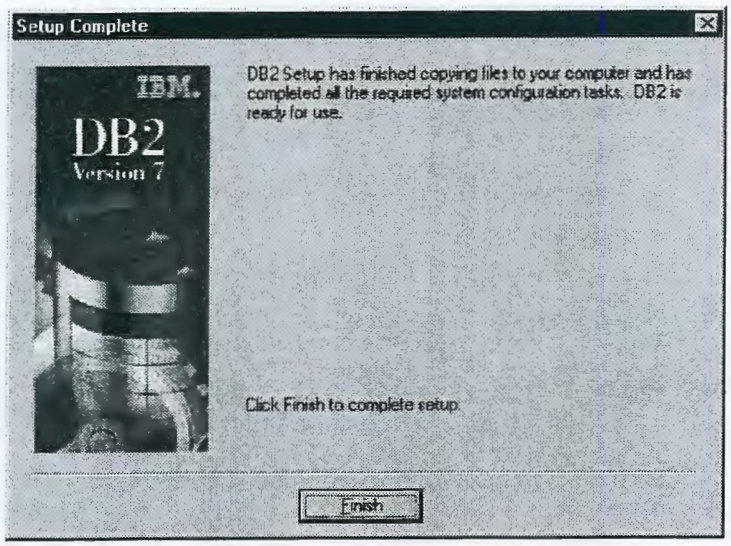


Figura 10. Painel Setup Complete

11. Inicie novamente o computador.
12. Após a reinicialização do computador, o DB2 estará totalmente instalado. Verifique se o DB2 foi instalado corretamente e veja se os serviços do DB2 foram iniciados. Na barra de tarefas, clique em:

    `Start → Settings →`
    `Control Panel → Administrative Tools → Services`
13. Além disso, você visualizará um painel **DB2 First Steps**. É possível praticar usando esse utilitário caso você não esteja familiarizado com o DB2. Quando terminar, feche esse painel.
14. Siga as etapas para fazer upgrade do DB2 com o FixPak 8. Consulte "Fazendo o Upgrade do DB2 com o FixPak 8".

Fazendo o Upgrade do DB2 com o FixPak 8

O FixPak 8 é requerido para o DB2 Versão 7.2. Existe um arquivo de upgrade do FixPak 8 disponível no seguinte Web site:

`http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report`

Siga estas etapas:

1. Efetue login no Windows como **db2admin** (ou outro ID de administrador do DB2).
2. Pare o DB2. Antes de parar o DB2, certifique-se de ter executado as seguintes ações:
   - Parar os serviços do DB2 Warehouse (se aplicável).
   - Parar qualquer outro aplicativo que acesse o DB2.
3. Copiar o arquivo zip para o disco rígido.
4. Descompactar o arquivo zip.
5. Executar o arquivo setup.exe. Siga as instruções nos painéis de instalação. Esse arquivo instala o upgrade sobre o DB2 existente.
6. Reinicie o sistema.

Fazendo o Upgrade dos Drivers JDBC do DB2 para a Versão 2

Para fazer o upgrade dos drivers JDBC do DB2, siga estas etapas:

1. Feche todos os navegadores.
2. Abra uma janela de prompt de comandos. É necessário desempenhar todas estas tarefas a partir dessa janela para verificar se existem mensagens de erro.
3. Altere a unidade e o diretório para a localização na qual você instalou os arquivos executáveis do DB2. O diretório padrão é C:\Arquivos de programas\SQLLIB.
4. Altere o diretório para java12.
5. Exiba o arquivo **em uso**, se houver. Se esse arquivo existir e indicar **JDBC 2.0**, significa que o driver JDBC correto já está instalado. Se o driver correto não estiver instalado, siga estas etapas:
   a. Pare todos os programas que possam estar utilizando o DB2.
   b. Pare o DB2 emitindo o comando: `db2stop`.
   c. Execute o arquivo em batch `usejdbc2.bat`. Certifique-se de que não existam mensagens de erro. Em caso positivo, corrija os erros e tente novamente.
   d. Inicie novamente o DB2 emitindo o comando: `db2start`.

O driver JDBC 2.0 já estará atualizado.

Etapa 5: Instale o Serviço SNMP

O Tivoli NetView é automaticamente instalado como parte da instalação do IBM Tivoli Storage Area Network Manager. Ele requer o serviço SNMP do Windows. Ao instalar o serviço SNMP, você precisará do CD do Windows 2000. Inicie novamente o computador depois de instalar o serviço SNMP. Se esse serviço não estiver instalado, o Tivoli NetView não será instalado. Se você já tiver o serviço SNMP instalado, poderá omitir essa etapa.

Siga estas etapas para instalar o serviço SNMP:

1. Na barra de tarefas, clique em:
   `Iniciar` → `Configurações` → `Painel de controle`

   A janela **Painel de controle** é exibida.
2. Dê um clique duplo no ícone **Adicionar ou remover programas**. A janela **Adicionar ou remover programas** é exibida.
3. Clique em **Adicionar ou remover componentes do Windows** à esquerda. A janela **Assistente de Componentes do Windows** é exibida.
4. Clique em **Ferramentas de gerenciamento e monitoria** e, em seguida, clique no botão **Detalhes**.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1518
Nº 3698
Doc.

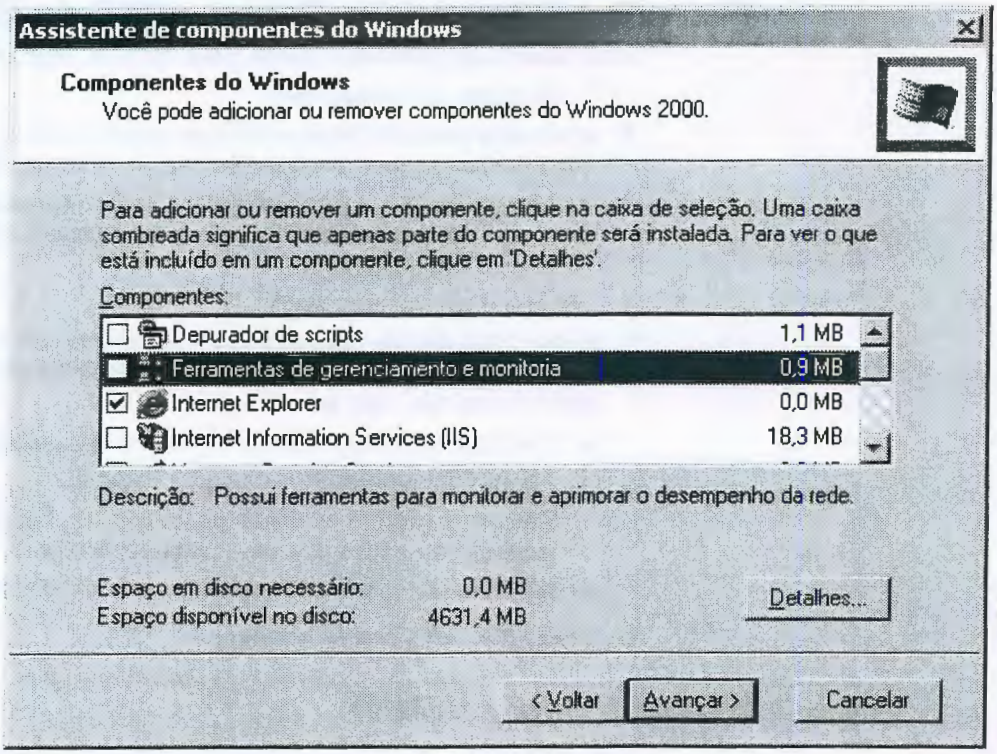


Figura 11. Assistente de Componentes do Windows

5. No painel **Ferramentas de Gerenciamento e Monitoria**, selecione **Simple Network Management Protocol** e, em seguida, clique em **OK**.

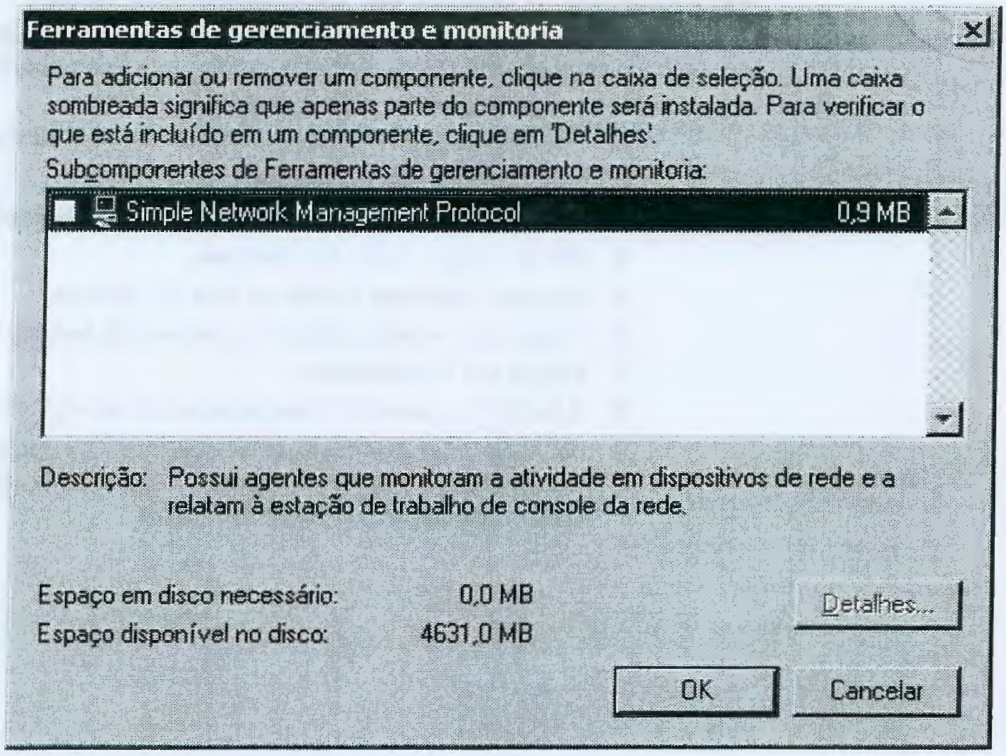


Figura 12. Painel Ferramentas de Gerenciamento e Monitoria

6. O painel **Assistente de componentes do Windows** é exibido. Clique em **Avançar** para continuar.
7. Se você não tiver o CD do Windows 2000 na unidade de CD–ROM, um prompt solicitará a inserção desse CD. Insira o CD do Windows 2000 na unidade de CD–ROM.
8. No painel **Assistente de componentes do Windows**, clique em **Concluir**.

Verificando o Nome da Comunidade SNMP

Após instalar o SNMP ou sempre que aplicar um pacote de serviços ou pacote de correção do Windows, verifique o nome da comunidade SNMP. Para verificar o nome da comunidade SNMP, siga essas etapas:

1. No desktop, dê um clique duplo no ícone **Meu Computador**.
2. Dê um clique duplo no **Painel de Controle**.
3. Dê um clique duplo em **Ferramentas Administrativas**.
4. Dê um clique duplo em **Serviços**.
5. Localize o **Serviço SNMP** na lista de serviços.
6. Clique com o botão direito do mouse em **Serviço SNMP**.
7. Clique em **Propriedades**.
8. É exibido o painel de Propriedades do Serviço SNMP.
9. Na guia Geral, certifique-se de que o tipo de Inicialização seja **Automática**.
10. Na guia Segurança, certifique-se de que o Nome da Comunicade seja **pública** com direitos de **SOMENTE LEITURA**.

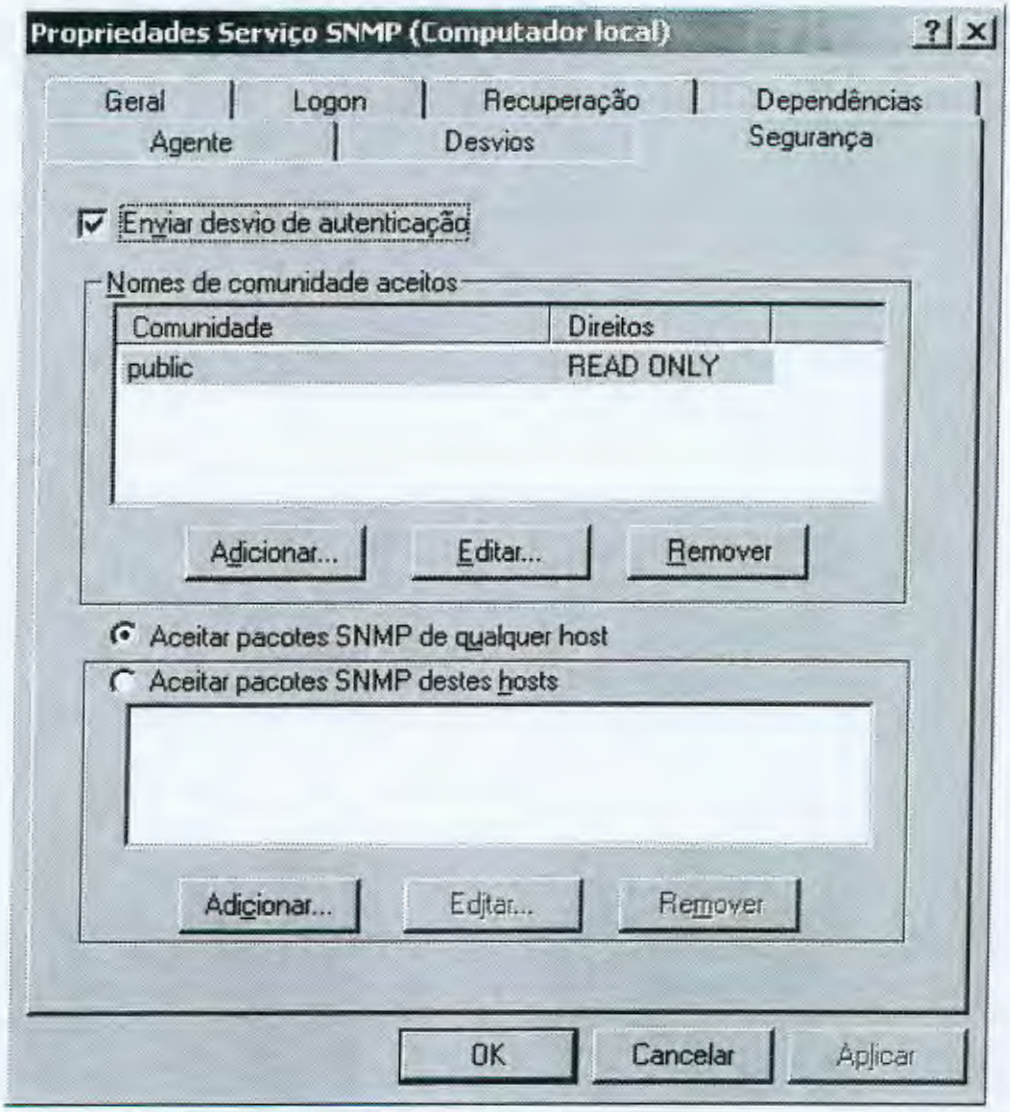


Figura 13. Painel de Propriedades do Serviço SNMP

11. Feche o painel de Propriedades do Serviço SNMP.

ROS nº 13/2005 CPMI CORREIOS
Fls. Nº 1520
Doc. 3698

Capítulo 4. Preparando-se para a Instalação (Gerenciador do AIX)

Antes de poder instalar o IBM Tivoli Storage Area Network Manager, existem várias etapas a serem concluídas. As seções a seguir descrevem essas etapas.

Etapa 1: Verificar Itens Necessários

O IBM Tivoli Storage Area Network Manager exige programas e serviços específicos para que você possa instalá-lo com êxito. A Tabela 9 fornece uma lista de programas e informações necessários para o IBM Tivoli Storage Area Network Manager (gerenciador). A Tabela 10 na página 36 fornece uma lista de programas e informações necessários para a instalação do console remoto. A Tabela 11 na página 36 fornece uma lista de informações necessárias para a instalação dos hosts gerenciados.

Tabela 9. Programas e Informações Necessários para a Instalação do Gerenciador do AIX

Número do Item	Item	Insira Informações Aqui
1	Nome do host completo do computador do gerenciador. Para verificar um nome de host completo, consulte "Etapa 2: Verificar o Nome do Computador" na página 37. Nomes de host fazem distinção entre maiúsculas e minúsculas (uma limitação do WebSphere). O gerenciador também exige um endereço IP estático.	
2	ID do administrador e senha DB2	
3	DB2 Versão 7.2 com FixPak 8 instalado. Se esse programa não estiver instalado, consulte a "Etapa 3: Instalar o DB2" na página 39.	
4	Uma faixa de sete números de porta (devem estar em ordem seqüencial). Certifique-se de que nenhum outro aplicativo esteja utilizando esses números de porta. Os números de porta padrão são de 9550 a 9556. Esses números de porta padrão são utilizados da seguinte maneira: **9550+0** Porta HTTP. **9550+1** Reservado. **9550+2** Reservado. **9550+3** Reservado. **9550+4** Porta NVDAEMON. **9550+5** Porta NVREQUESTER. **9550+6** Porta SNMPTrapPort na qual são obtidos eventos encaminhados do Tivoli NetView.	

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1521
Doc. 3698

As informações na tabela a seguir destinam-se ao console remoto no Windows.

Tabela 10. Programas e Informações Necessários para a Instalação do Console Remoto

Número do Item	Item	Insira Informações Aqui
1	Tivoli NetView versão 7.1.3. Se esse programa não estiver instalado, o IBM Tivoli Storage Area Network Manager o instalará automaticamente. Se o Tivoli NetView versão 7.1.3 estiver instalado, será configurado pelo programa de instalação. Se o Tivoli NetView versão 7.1.1 estiver instalado, será feito o upgrade para 7.1.3.	
2	Serviço SNMP. Para instalar o Serviço SNMP, consulte a "Etapa 5: Instale o Serviço SNMP" na página 29.	
3	Serviço de Planejamento (Windows 2000)	
4	Número da porta e nome do host completo do gerenciador. Para verificar o nome do host completo, consulte "Verificando Nomes de Host Completos" na página 204.	
5	Uma faixa de seis números de porta (devem estar em ordem seqüencial). Certifique-se de que nenhum outro aplicativo esteja utilizando esses números de porta. Os números de porta padrão são de 9560 à 9565. Esses números de porta padrão são utilizados da seguinte maneira: **9560+0** Porta HTTP. **9560+1** Reservado. **9560+2** Porta do Servidor Local do Tomcat. **9560+3** Porta Warp do Tomcat. **9560+4** Porta NVDAEMON. **9560+5** Porta NVREQUESTER.	
6	Senha de autenticação do host	

Tabela 11. Programas e Informações Necessários para a Instalação do Agente no Host Gerenciado

Número do Item	Item	Insira Informações Aqui
1	Número da porta e nome do host completo do gerenciador. Para verificar o nome do host completo, consulte "Verificando Nomes de Host Completos" na página 204.	

Tabela 11. Programas e Informações Necessários para a Instalação do Agente no Host Gerenciado (continuação)

Número do Item	Item	Insira Informações Aqui
2	Uma faixa de quatro números de porta (devem estar em ordem seqüencial). Certifique-se de que nenhum outro aplicativo esteja utilizando esses números de porta. Os números de porta padrão são de 9570 a 9573. Esses números de porta padrão são utilizados da seguinte maneira: **9570+0** Porta HTTP. **9570+1** Reservado. **9570+2** Porta do Servidor Local do Tomcat. **9570+3** Porta Warp do Tomcat.	
3	É necessário ter as correções atuais do sistema operacional para oferecer suporte ao JRE 1.3.1. O JRE 1.3.1 é instalado pelo programa de instalação.	
4	Senha de autenticação do host	

Existem algumas diferenças na instalação dos gerenciadores do Windows e AIX. As diferenças são:

- O Tivoli NetView não está instalado ou não é suportado no gerenciador do AIX. Se desejar ver a exibição da GUI no IBM Tivoli Storage Area Network Manager, instale o console remoto no Windows 2000 ou Windows XP.

Etapa 2: Verificar o Nome do Computador

O IBM Tivoli Storage Area Network Manager exige nomes de host completos para o gerenciador, os hosts gerenciados e o console remoto. Nomes de host fazem distinção entre maiúsculas e minúsculas. Essa é uma limitação do WebSphere. O gerenciador também exige um endereço IP estático. Para verificar o nome do computador no AIX, consulte as informações a seguir.

Para verificar se seu computador está utilizando um endereço IP estático, execute este comando:

```
lssrc -g tcpip
```

Verifique se o daemon **dhcpcd** *não* está sendo executado. Um exemplo de saída é mostrado a seguir indicando que o daemon **dhcpcd** está inoperante.

```
Subsistema      Grupo           PID     Status
 inetd          tcpip           7226    ativo
 snmpd          tcpip           7744    ativo
 dpid2          tcpip           8260    ativo
 hostmibd       tcpip           7484    ativo
 rwhod          tcpip                   inoperante
 xntpd          tcpip                   inoperante
 dhcpcd         tcpip                   inoperante
```

A ordem de pesquisa de nomes de domínio padrão é a seguinte:

1. Servidor DNS (Domain Name System)
2. NIS (Network Information Service)
3. Arquivo /etc/hosts local

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1522
3698
Doc.

Se o arquivo /etc/resolv.conf não existir, o arquivo /etc/hosts será utilizado. Se apenas o arquivo /etc/hosts for utilizado, o nome completo do computador deverá ser o primeiro nome listado após o endereço IP.

Verifique se o arquivo /etc/resolv.conf existe e se contém as informações apropriadas, como:

```
domínio minhadivisão.minhaempresa.com
servidordenomes 123.123.123.123
```

Se o NIS estiver instalado, o arquivo /etc/irs.conf substituirá o padrão do sistema. Essa variável contém as seguintes informações:

```
hosts = bind,local
```

O arquivo /etc/netsvc.conf, se houver, substituirá o arquivo /etc/irs.conf e o padrão do sistema. Essa variável contém as seguintes informações:

```
hosts = bind,local
```

Se a variável de ambiente NSORDER estiver definida, substituirá todos os arquivos precedentes. Essa variável contém as seguintes informações:

```
export NSORDER=bind,local
```

Etapa 3: Instalar o DB2

Instale o DB2 Versão 7.2. O IBM Tivoli Storage Area Network Manager cria tabelas do DB2 para seus dados. Instale o DB2 no computador do gerenciador.

Nota: Convém dedicar o DB2 para o IBM Tivoli Storage Area Network Manager. Fazer com que outros aplicativos utilizem o DB2 pode prejudicar o desempenho.

Se você tiver o DB2 Enterprise Edition Versão 7.2 instalado, poderá omitir este procedimento de instalação e seguir as etapas em "Fazendo o Upgrade do DB2 com o FixPak 8" na página 46. Caso contrário, instale o DB2. Para isso, siga as etapas em "Fazendo o Upgrade do DB2 com o FixPak 8" na página 46.

Para instalar o DB2, siga estas etapas.

1. Efetue login como usuário root.
2. Inicie uma sessão do terminal.
3. Carregue o CD do IBM DB2 na unidade de disco de CD–ROM e monte o CD. Se não houver um diretório de CD-ROM, será necessário criá-lo.

   ```
   # mkdir cdrom    (para criar o diretório cdrom)
   # mount -v'cdrfs' -r'' /dev/cd0 /cdrom
   ```

   Observe que a opção –r é acompanhada de duas aspas.
4. Vá para o diretório do CD–ROM:

   ```
   # cd cdrom
   ```
5. Inicie o Utilitário de Instalação do DB2 executando o seguinte comando:

   ```
   # ./db2setup
   ```
6. O painel Utilitário de Instalação do DB2 é exibido. Realce o botão **Instalar** à direita de **Selecionar os produtos e seus componentes, selecione Instalar** e pressione **Enter**.

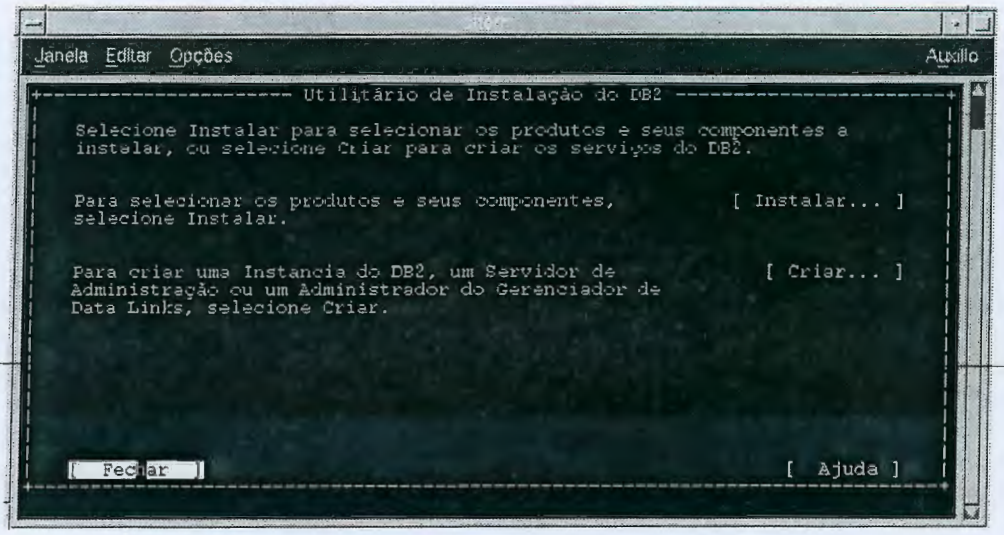


Figura 14. Painel do Utilitário de Instalação do DB2

7. O painel **DB2 Select Products** é exibido. Realce e pressione **Enter** para selecionar os seguintes itens:
   - Cliente de Administração do DB2
   - DB2 UDB Enterprise Edition
   - DB2 Connect Enterprise Edition

   Realce o Biblioteca do Produto DB2. Em seguida, realce **Personalizar** e pressione **Enter**.

Dicas de Navegação
- Pressione **Tab** para mover-se entre as opções e os campos disponíveis.
- Realce e pressione **Enter** para selecionar uma opção.

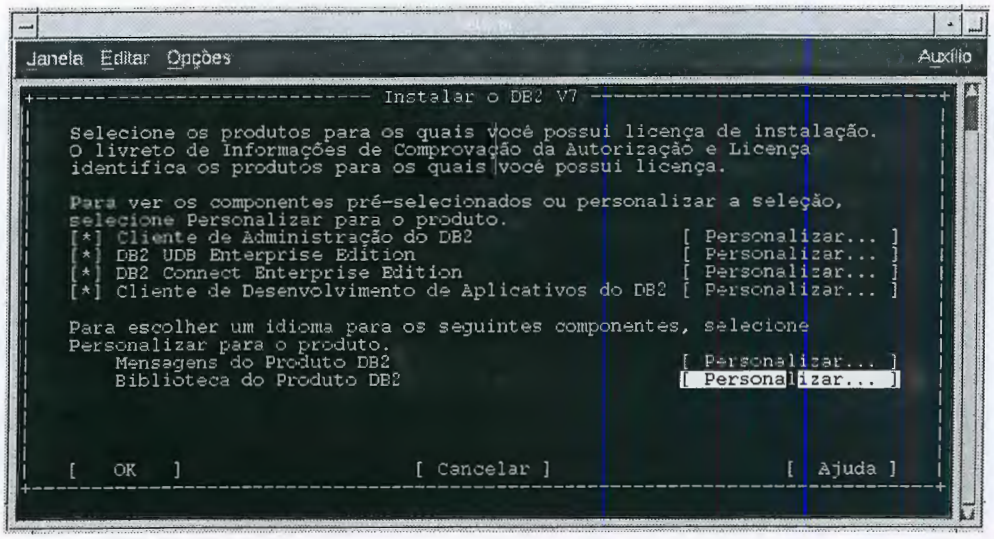


Figura 15. Painel DB2 Select Products

8. O painel do Biblioteca do Produto DB2 é exibido. Realce a opção apropriada para o seu locale. Realce **OK** e pressione **Enter**.

Figura 16. Painel do Biblioteca do Produto DB2

9. Você verá o painel do DB2 Select Products (Figura 15 na página 40). Realce **OK** *novamente* e pressione **Enter**.
10. O painel Criar Serviços do DB2 é exibido. Certifique-se de que Não Criar uma Instância do DB2 e Não Criar o Servidor de Administração estejam selecionados. Realce **OK** e pressione **Enter**.

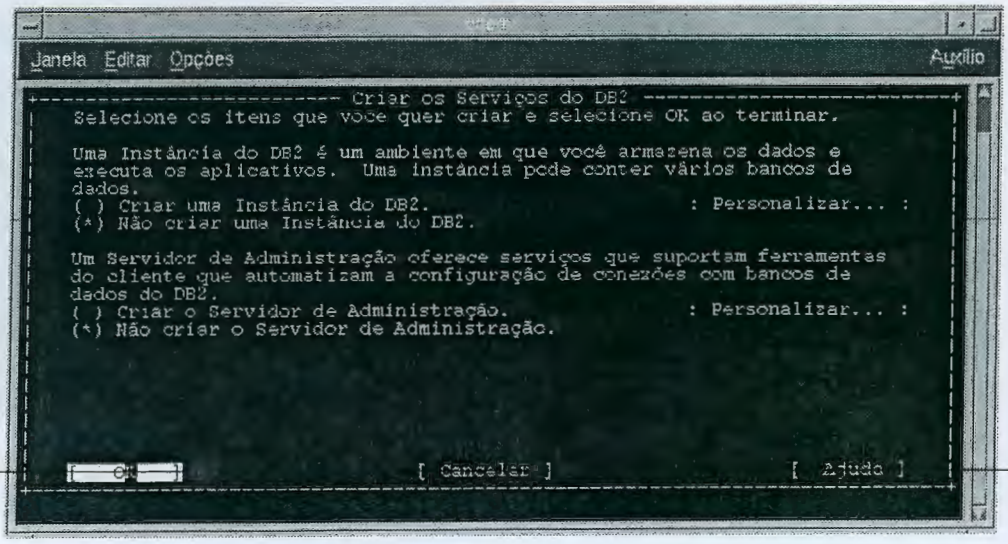


Figura 17. Painel Criar Serviços do DB2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1524
Doc. 3698

11. Você verá uma Mensagem de aviso exibida para a Instância do DB2. Realce **OK** e pressione **Enter**.

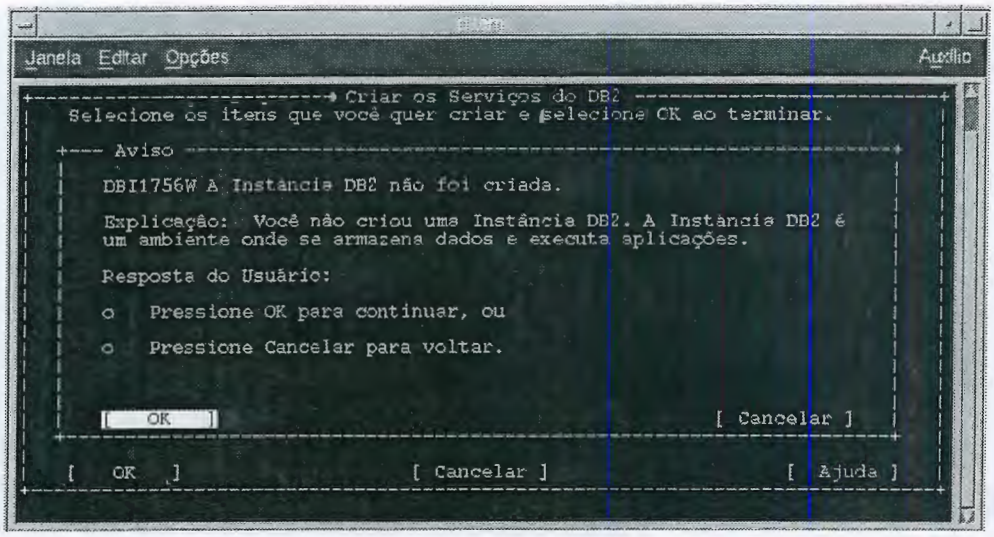


Figura 18. Mensagem de Aviso para a Instância do DB2

12. Você verá uma Mensagem de aviso para o servidor de administração. Realce **OK** e pressione **Enter**.

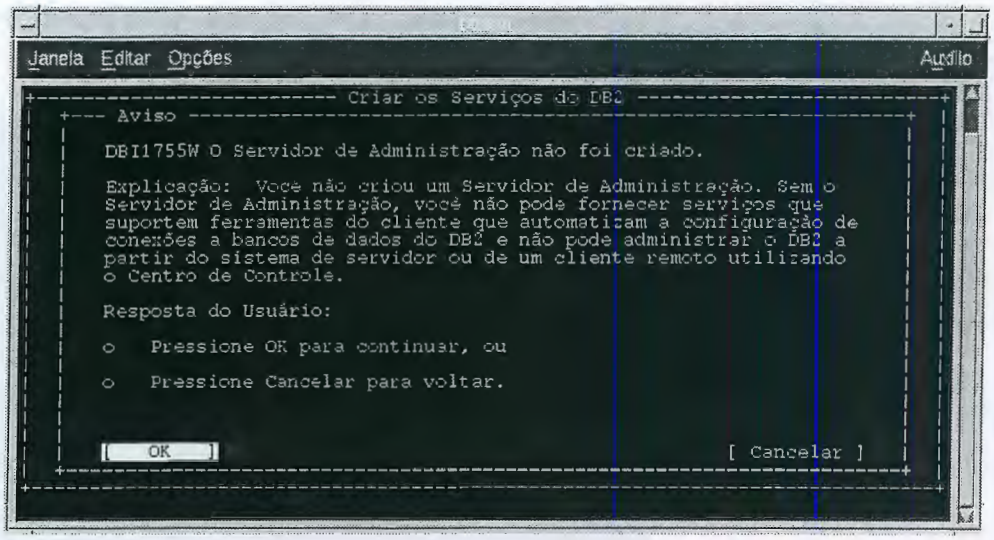


Figura 19. Mensagem de Aviso para o Servidor de Administração

13. O painel Relatório de Resumo é exibido. Realce **Continuar** e pressione **Enter**.

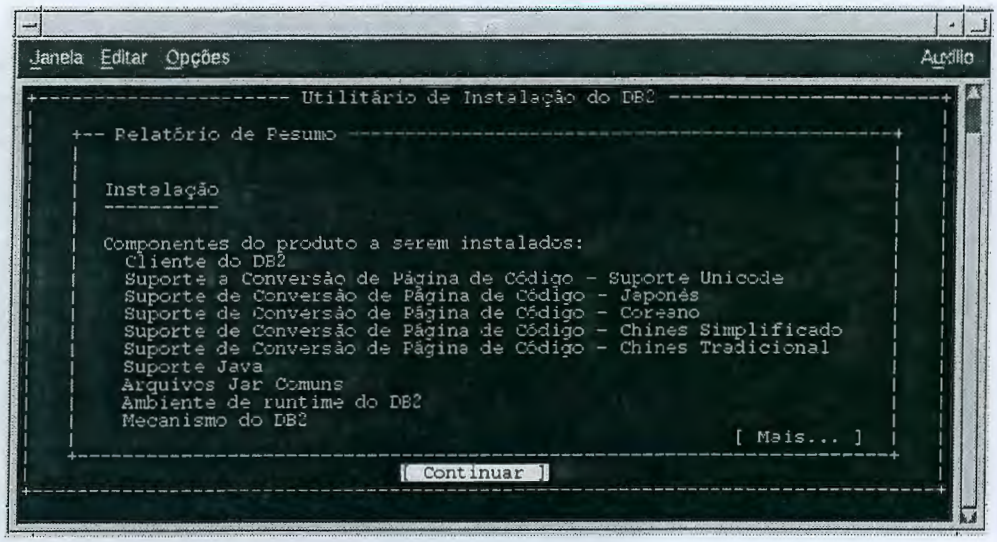


Figura 20. Painel Relatório de Resumo

14. Você verá uma mensagem de aviso informando uma última chance de parar. Esta é uma mensagem normal. Realce **OK** para instalar e pressione **Enter**.

Figura 21. Mensagem de Aviso

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1525
Doc. 3698

15. Você verá uma mensagem para instalação. Deixe o programa continuar a instalação. Dependendo da velocidade de seu processador, isto pode demorar até 15 minutos.

Figura 22. Messagem para Instalação

16. Você verá uma mensagem, "Concluído com êxito." Realce **OK** e pressione **Enter**.

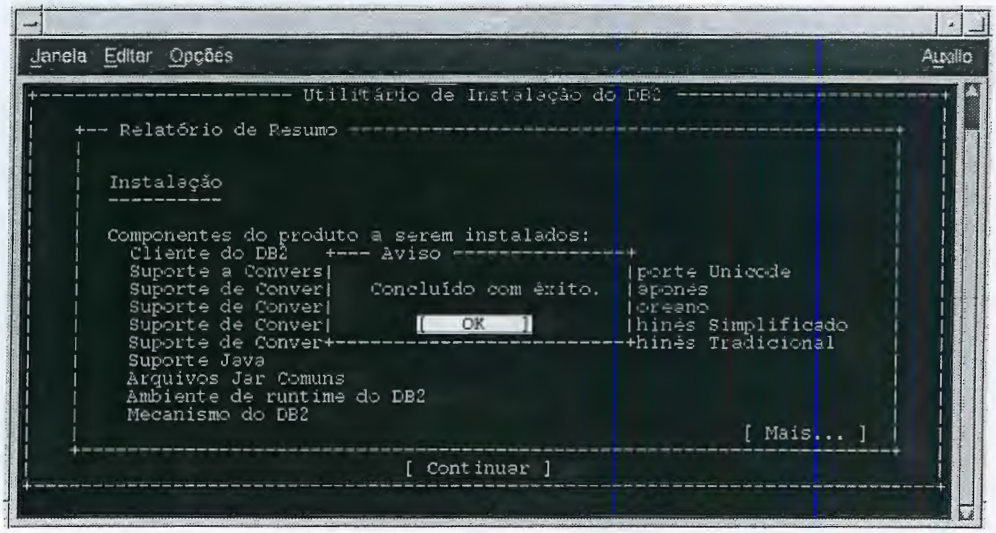


Figura 23. Mensagem "Concluído com êxito"

17. Você verá uma janela pop–up perguntando se você deseja registrar o software DB2. Clique em **Sair** e depois em **Sim**.
18. No painel Relatório de Status, visualize o log para certificar-se de que todos os componentes foram instalados com êxito. Realce **OK** e pressione **Enter**.

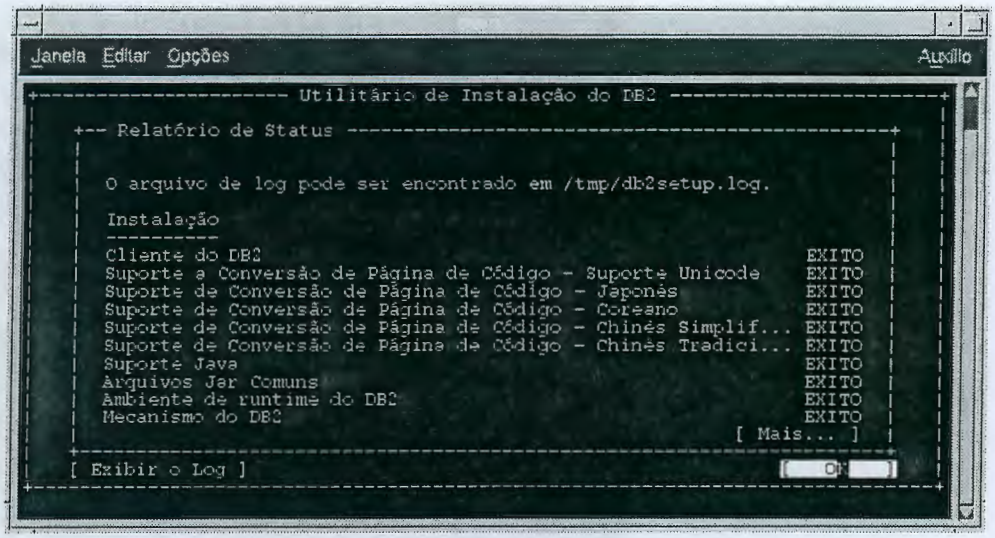


Figura 24. Painel Relatório de Status

19. Você verá o painel do Utilitário de Instalação do DB2 (Figura 14 na página 39). Realce **Fechar** e pressione **Enter** para sair do **db2setup**.
20. Você verá a seguinte mensagem:

    `A Instância do DB2 não foi criada.`

    Realce **OK** e pressione **Enter**.
21. Você verá a seguinte mensagem:

    `O Servidor de Administração não foi criado.`

    Realce **OK** e pressione **Enter**.
22. Você verá o painel do Utilitário de Instalação do DB2. Realce **OK** e pressione **Enter**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1326
Nº 3698
Doc

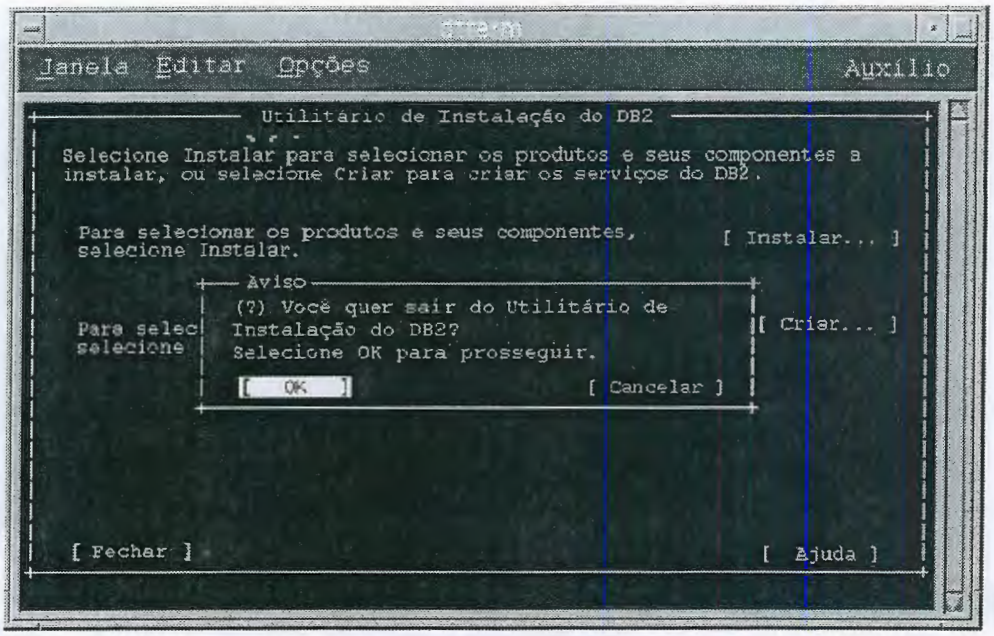


Figura 25. Painel do Utilitário de Instalação do DB2

23. Realce **Fechar** e pressione **Enter** para sair do Utilitário de Instalação do DB2.

Fazendo o Upgrade do DB2 com o FixPak 8

O FixPak 8 é requerido para o DB2 Versão 7.2. Você pode obter os fixpacks no Web site a seguir. Utilize este procedimento para instalar o fixpack.

```
http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/
download.d2w/report
```

Siga estas etapas:

1. Faça download do fix pack do Web site. Leia o arquivo README fornecido junto.
2. Assegure-se de que efetuou login na máquina com autoridade superusuário (root).
3. Navegue para o diretório que contém o arquivo tar transferido por download.
4. Descompacte o arquivo tar:

   ```
   # uncompress nome_do_arquivo.tar.Z
   ```

   O nome do arquivo tar é o seguinte:
   - FixPak 8 – FP8_U484610.tar.Z
5. Descompacte o arquivo que foi transferido por download para extrair os pacotes do DB2 utilizando o comando **tar**:

   ```
   # tar -xvf nome_do_arquivo.tar
   ```
6. Pare o DB2. Antes de parar o DB2, certifique-se de ter executado as seguintes ações:
   - Parar os serviços do DB2 Warehouse (se aplicável).
   - Parar qualquer outro aplicativo que acesse o DB2.
7. Execute o SMIT para atualizar todos os arquivos, digitando o seguinte comando:

   ```
   # smit update_all
   ```

8. No campo **Dispositivo de ENTRADA/diretório do software**, especifique o nome completo do diretório que contém os arquivos descompactados e preparados do FixPak. Clique em **OK**.
9. Aceite as opções padrão do SMIT para atualizar o DB2 e clique em **OK**.
10. Você verá a mensagem "Tem certeza?" Clique em **OK** para instalar o fix pack.
11. Quando este processo estiver concluído, saia do SMIT.

Criando uma Instância do Banco de Dados e o Servidor de Administração

O servidor de administração não possui nenhum banco de dados. O proprietário da Instância do DB2 possui o banco de dados e tem permissão de criar ou eliminar bancos de dados do DB2.

Execute as seguintes etapas para criar uma Instância do DB2 e os recursos que ela requer:

1. Assegure-se de que efetuou login na máquina com privilégios de superusuário (root).
2. Vá para o diretório que contém o Utilitário de Instalação do DB2:

   ```
   cd /usr/lpp/<programa_DB2>/install/
   ```

   em que *programa_DB2* é o nome do programa DB2. Um exemplo é db2_07_01.
3. Inicie o Utilitário de Instalação do DB2, digitando o seguinte comando:

   ```
   # ./db2setup
   ```


Fls. Nº 1527
Doc

4. O painel Utilitário de Instalação do DB2 é exibido. Realce o botão **Criar** à direita de **Para criar uma instância de DB2, um Servidor de Administração ou um Administrador de Gerenciador de Links de Dados, selecione Criar.** Pressione **Enter**.

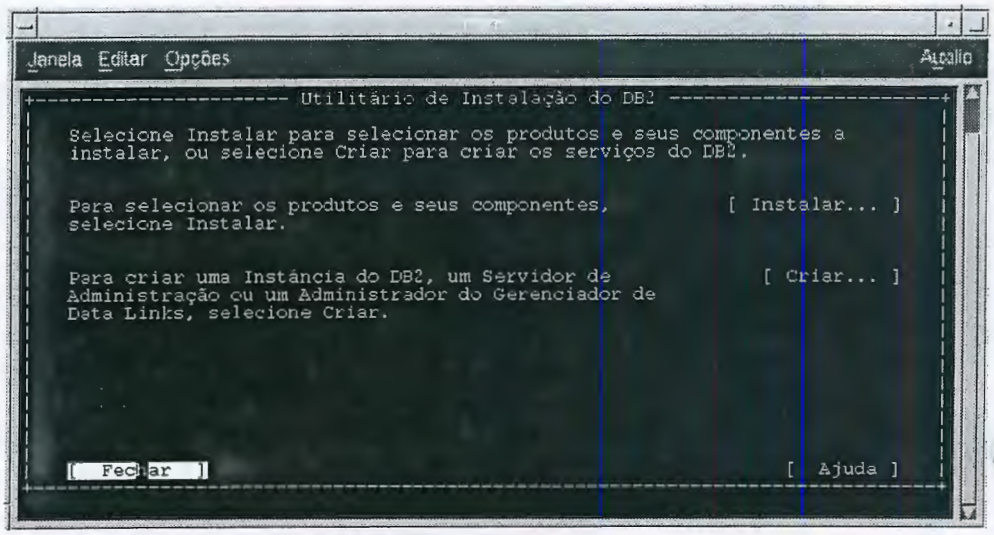


Figura 26. Painel do Utilitário de Instalação do DB2

5. O painel Criar Serviços do DB2 é exibido. Realce a opção **Criar uma Instância do DB2** e pressione **Enter**.

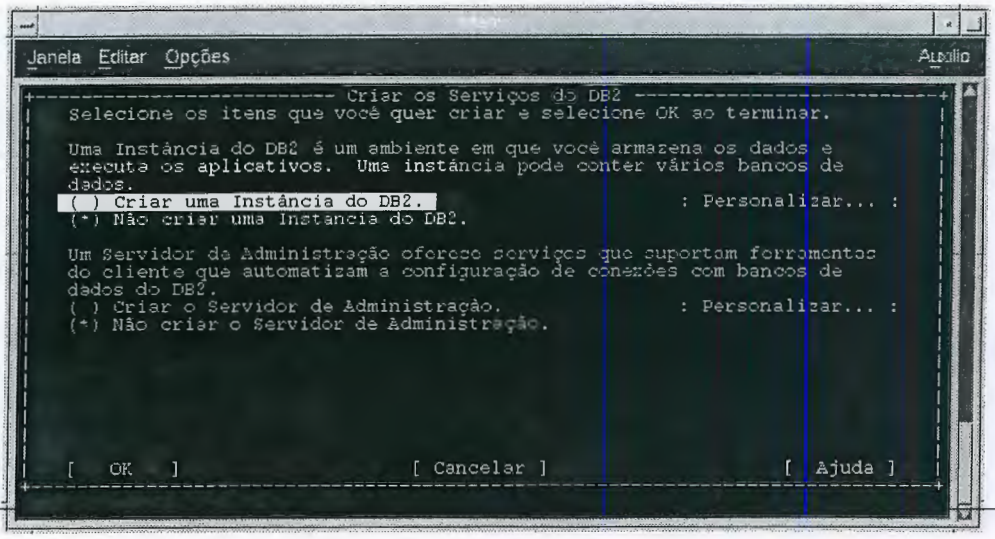


Figura 27. Painel Criar Serviços do DB2

10243
VA.

6. O painel Instância do DB2 é exibido. Insira estas informações para os seguintes campos:
   - Nome do Usuário – aceite o valor padrão, **db2inst1**.
   - ID do Usuário – insira um ID do usuário ou aceite o ID do usuário padrão assegurando que a opção **Utilizar UID padrão** tenha um * (asterisco) ao seu lado.
   - Nome do Grupo – aceite o valor padrão, **db2iadm1**.
   - ID do Grupo – insira um ID do grupo ou aceite o ID do grupo padrão assegurando que a opção **Utilizar GID padrão** tenha um asterisco ao seu lado.
   - Diretório Inicial – aceite o valor padrão, **/home/db2inst1**.
   - Senha – insira a mesma senha para o usuário neste campo e no campo **Verificar Senha**. O DB2 requer uma senha de oito caracteres ou menos.
   - Realce **OK** e pressione **Enter**.

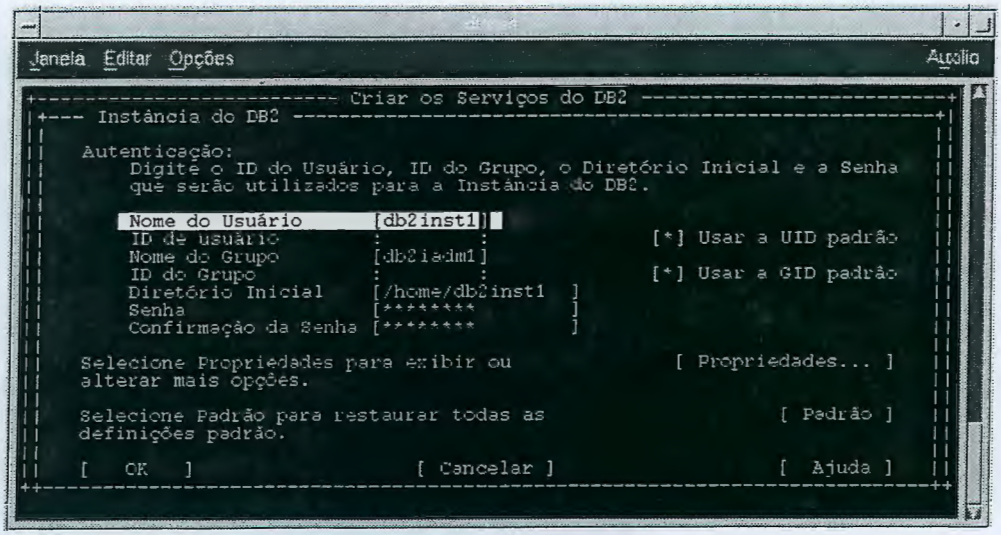


Figura 28. Painel Instância do BD2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1528
Doc. 3698

7. O painel Usuário Delimitado é exibido. Insira estas informações para os seguintes campos:
   - Nome do Usuário – aceite o valor padrão, **db2fenc1**.
   - ID do Usuário – insira um ID do usuário ou aceite o ID do usuário padrão assegurando que a opção **Utilizar UID padrão** tenha um * (asterisco) ao seu lado.
   - Nome do Grupo – aceite o valor padrão, **db2fadm1**.
   - ID do Grupo – insira um ID do grupo ou aceite o ID do grupo padrão assegurando que a opção Utilizar GID padrão tenha um * (asterisco) ao seu lado.
   - Diretório Inicial – insira um diretório inicial ou aceite o valor padrão, **/home/db2fenc1**.
   - Senha – insira a mesma senha para o usuário neste campo e no campo **Verificar Senha**. O DB2 requer uma senha de oito caracteres ou menos.
   - Realce **OK** e pressione **Enter**.

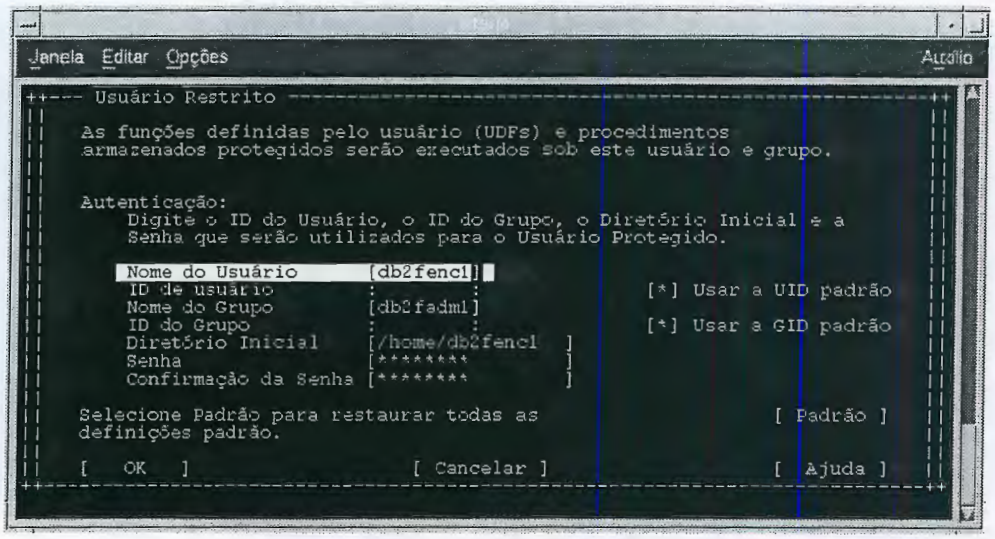


Figura 29. Painel Usuário Delimitado

8. O painel Banco de Dados de Controle do DB2 Warehouse é exibido. Realce **Não configurar o Banco de Dados de Controle do DB2 Warehouse** e pressione **Enter**. Realce **OK** e pressione **Enter**.

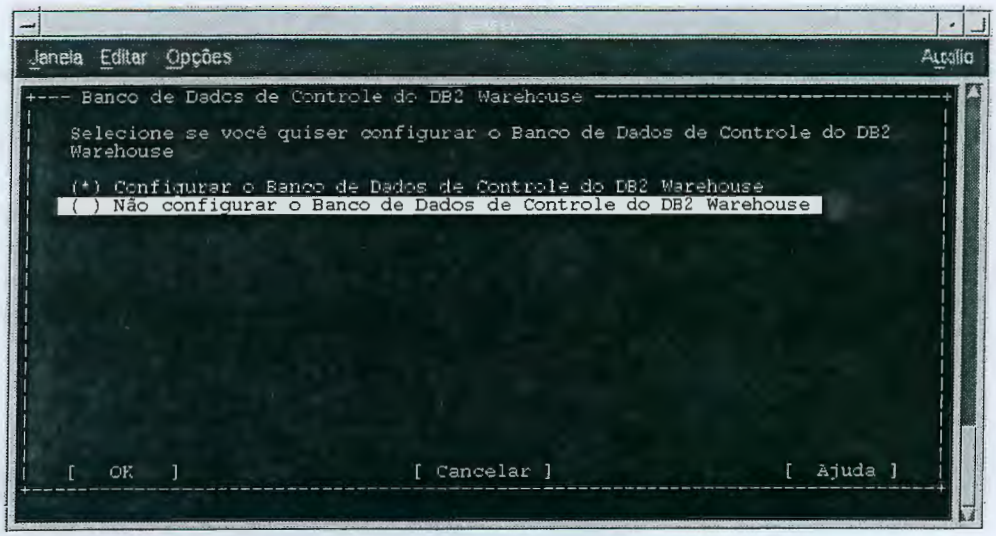


Figura 30. Painel Banco de Dados de Controle do DB2 Warehouse

9. O painel Criar Serviços do DB2 é exibido. Realce **Criar o Servidor de Administração** e pressione **Enter**.

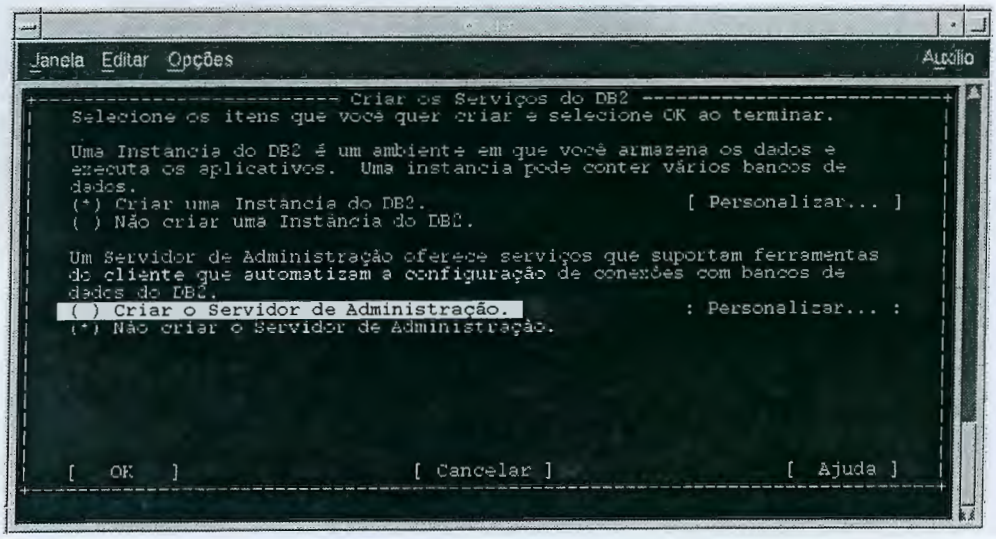


Figura 31. Painel Criar Serviços do DB2

RQS nº 03/2005
CPMI
Fls Nº 1529
3698
Doc

10. O painel Servidor de Administração é exibido. Insira estas informações para os seguintes campos:
    - Nome do Usuário – aceite o valor padrão, **db2as**.
    - ID do Usuário – insira um ID do usuário ou aceite o ID do usuário padrão assegurando que a opção **Utilizar UID padrão** tenha um * (asterisco) ao seu lado.
    - Nome do Grupo – aceite o valor padrão, **db2asgrp**.
    - ID do Grupo – insira um ID do grupo ou aceite o ID do grupo padrão assegurando que a opção Utilizar GID padrão tenha um * (asterisco) ao seu lado.
    - Diretório Inicial – insira um diretório inicial ou aceite o valor padrão, **/home/db2as**.
    - Senha – insira a mesma senha para o usuário neste campo e no campo **Verificar Senha**. O DB2 requer uma senha de oito caracteres ou menos.
    - Realce **OK** e pressione **Enter**.

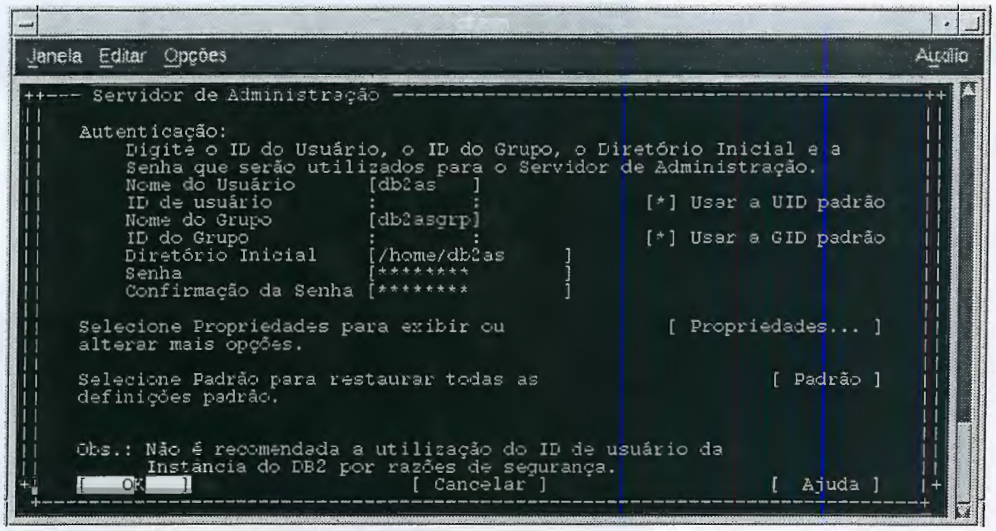


Figura 32. Painel Servidor de Administração

11. É exibido um aviso informando o valor que está sendo criado para a variável de ambiente DB2SYSTEM. Realce **OK** e pressione **Enter**.

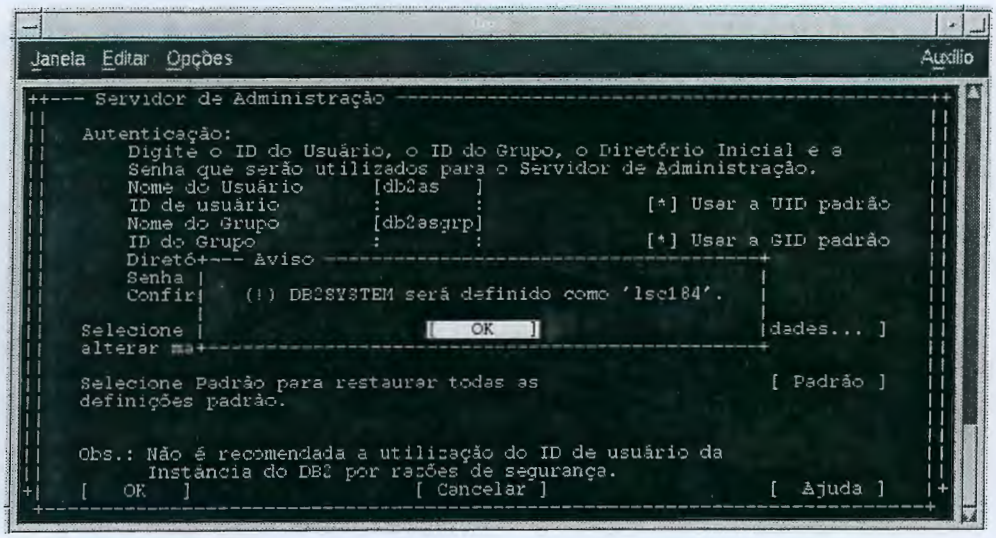


Figura 33. Painel Aviso

12. O painel Criar Serviços do DB2 é exibido. Realce **OK** e pressione **Enter**.

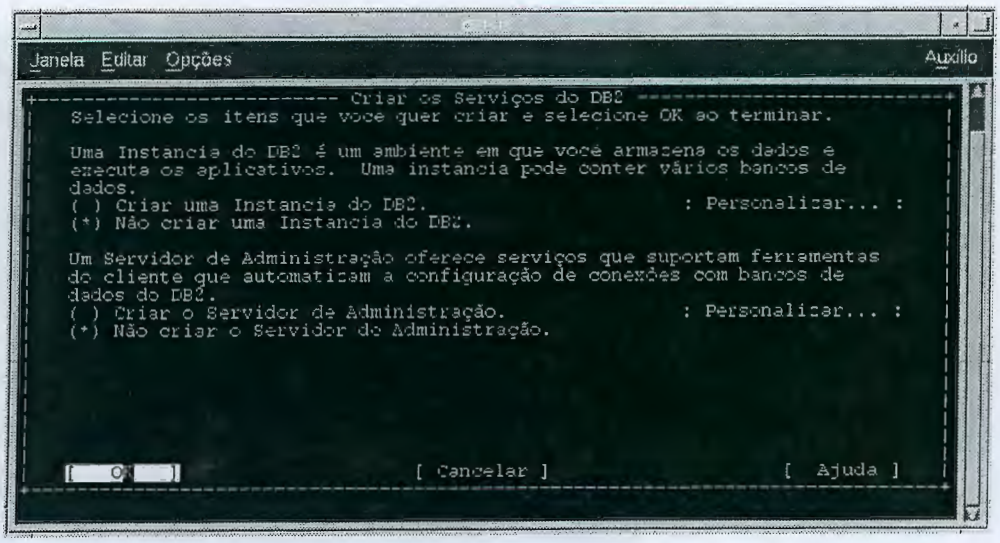


Figura 34. Painel Criar Serviços do DB2

RQS nº 03/2005
CPMI - CORREIOS
Fls Nº 1530
Doc. 3698

13. O painel Relatório de Resumo é exibido. Verifique as informações no Relatório de Resumo. Quando concluir, realce **Continuar** e pressione **Enter**.

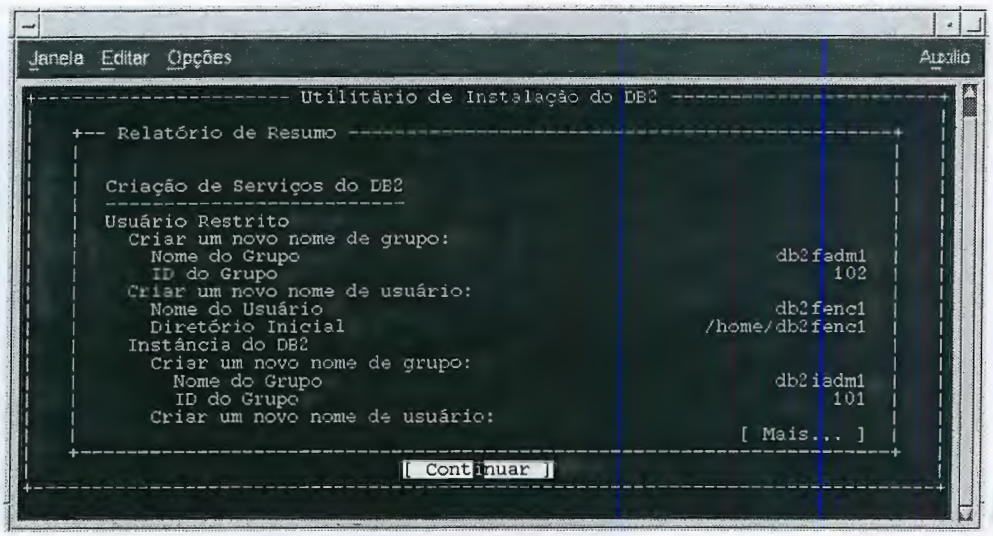


Figura 35. Painel Relatório de Resumo

14. Uma mensagem de aviso é exibida com a opção de cancelar os processos de configuração. Para continuar, realce **OK** e pressione **Enter**.

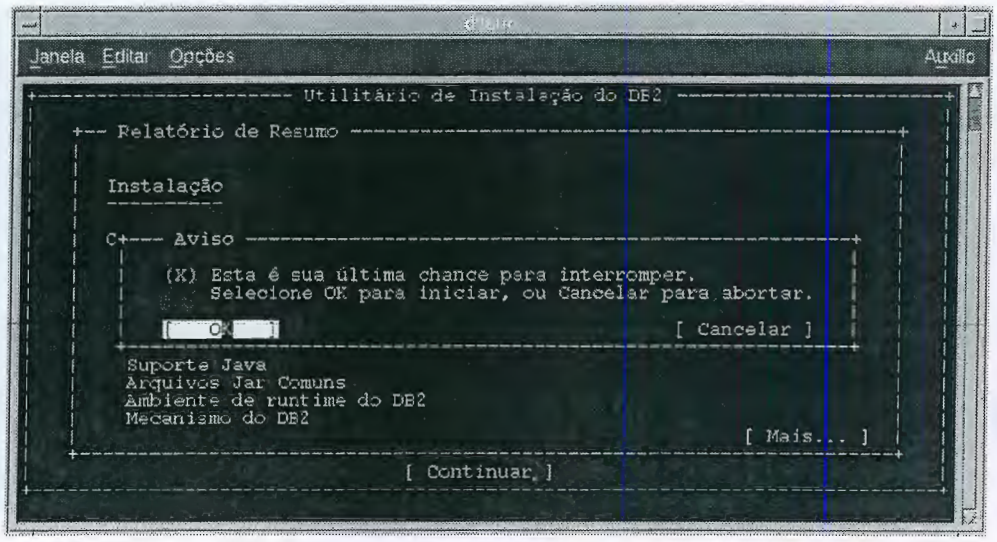


Figura 36. Mensagem de Aviso

15. Uma mensagem informa sobre a conclusão bem-sucedida dos processos. Realce **OK** e pressione **Enter**.

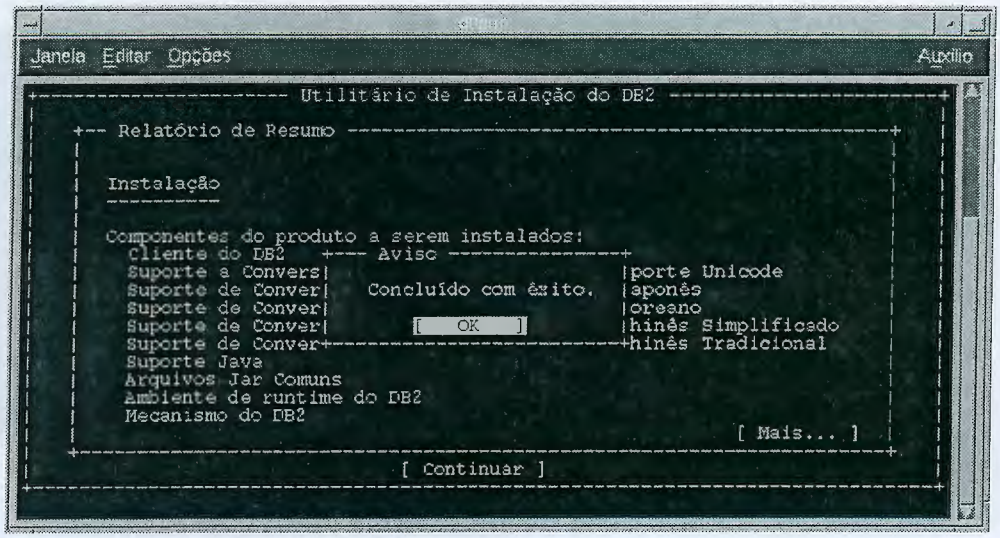


Figura 37. Mensagem Concluído com êxito

16. O painel Relatório de Status informa sobre os sucessos e defeitos do processo. Visualize o arquivo de logs para obter informações sobre como corrigir determinados defeitos. Realce **OK** e pressione **Enter** para fechar o Relatório de Status.
17. No painel do Utilitário de Instalação do DB2, realce **Fechar** e pressione **Enter**.
18. É exibida uma janela que solicita o seguinte:

    `Deseja sair do Utilitário de Instalação do DB2?`

    Realce **OK** e pressione **Enter**. A instalação do DB2 agora está concluída.
19. Verifique se o usuário **root** é um membro do grupo de servidores de administração denominado **db2asgrp** executando estas etapas:
    a. Chame o SMIT para alterar as características do usuário inserindo **smit**. Vá para estes painéis:

       `Segurança & Usuário`
       `Grupos`
       `Alterar ou Mostrar Características de um Grupo`

    b. O painel Alterar Atributos do Grupo é exibido. Para o Nome do Grupo, insira **db2asgrp**. Clique em **OK**. Se o campo Lista de ADMINISTRADORES não exibir **root**, adicione **root** à lista e clique em **OK**.

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 1531
Doc. 3698

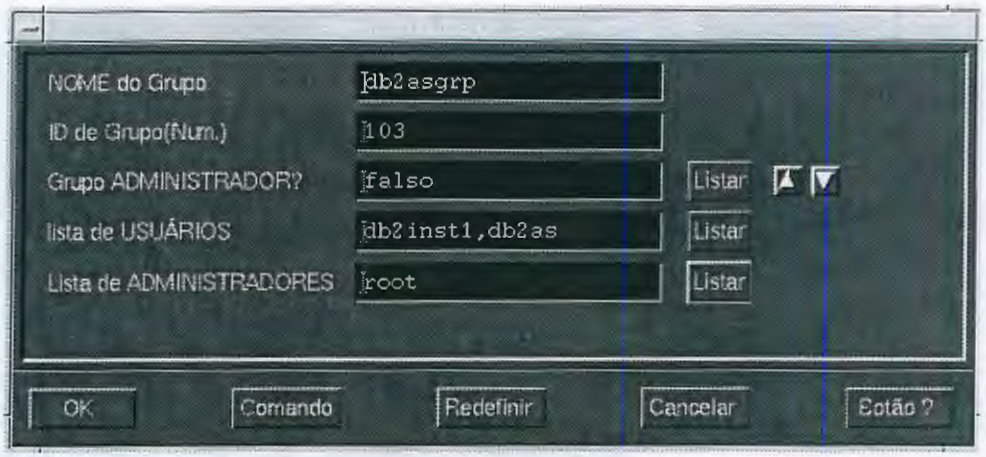


Figura 38. Painel Alterar Atributos do Grupo para db2asgrp

c. O painel Alterar Atributos do Grupo mostra que o procedimento está concluído. Clique em **Concluído**.

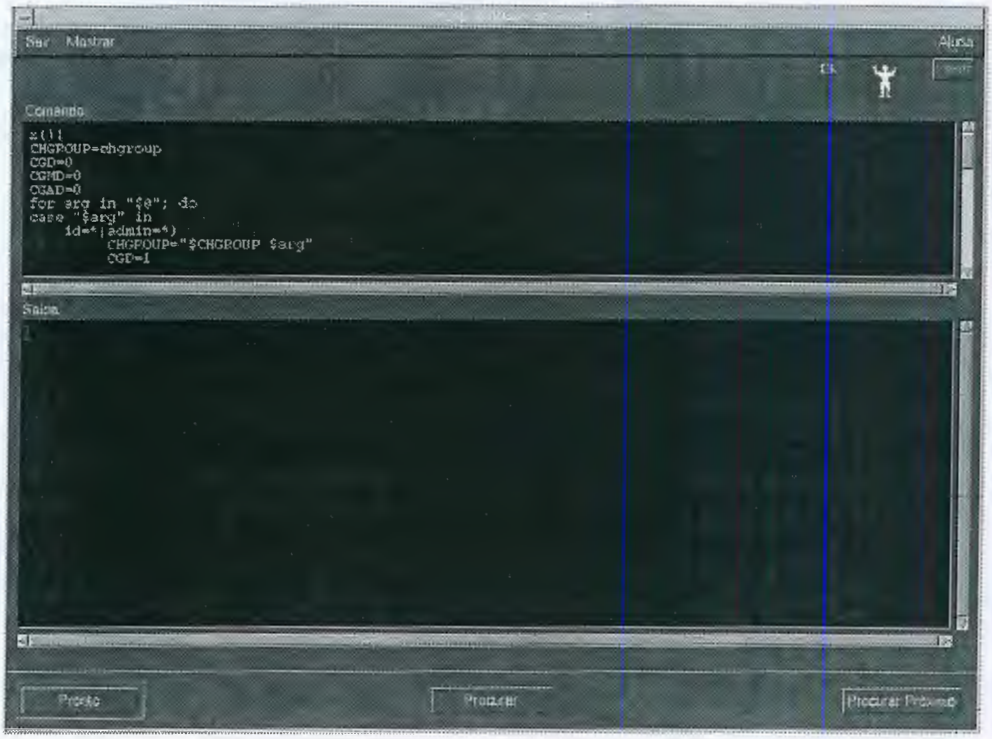


Figura 39. Painel Alterar Atributos do Grupo para db2asgrp - concluído

d. Clique em **Cancelar** no painel Alterar Atributos do Grupo. Esse procedimento exibe o painel Alterar ou Mostrar Características de um Grupo. Selecione isto novamente.

e. O painel Alterar Atributos do Grupo é exibido novamente. Para o Nome do Grupo, insira **db2iadm1** e clique em **OK**. Se **root** não aparecer no campo Lista de USUÁRIOS, adicione **root** e clique em **OK**.

10235
A.

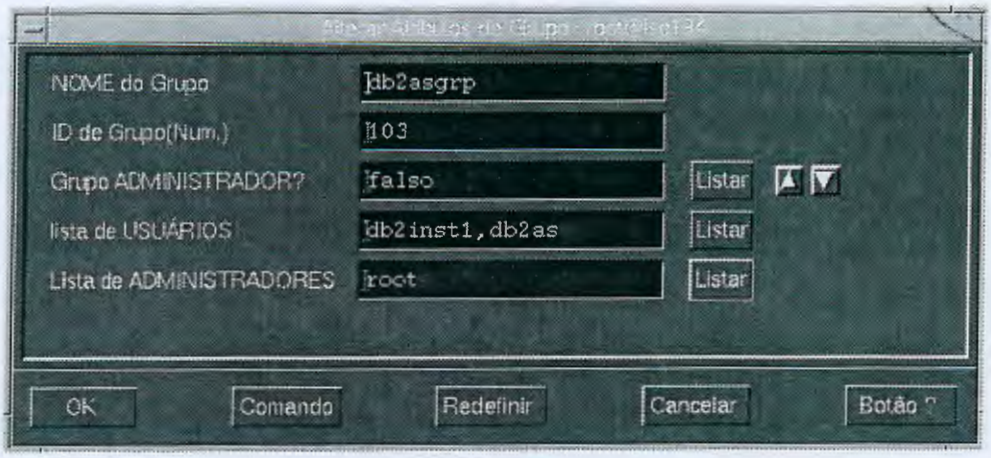


Figura 40. Painel Alterar Atributos do Grupo para db2iadm1

f. Clique em **Concluído** quando o procedimento estiver concluído.

g. Quando o processo estiver concluído, saia do SMIT.

Atualizando a Variável de Ambiente EXTSHM

Para atualizar o número de segmentos da memória compartilhada para um processo, siga as etapas a seguir para atualizar o perfil do usuário. Observe que se você reinstalar o DB2, deverá executar estas etapas novamente.

Siga estas etapas:

1. Inclua as seguintes informações em ~db2inst1/sqllib/userprofile:

```
EXTSHM=ON
export EXTSHM
db2set DB2ENVLIST=EXTSHM
```

2. Você pode efetuar login como o proprietário da instância do DB2, por exemplo:

```
su - db2inst1
```

   Ou você pode utilizar este exemplo para executar o comando do DB2. O db2profile chama o perfil do usuário.

```
. ~db2inst1/sqllib/db2profile
```

3. Parar o DB2:

```
db2stop
```

4. Iniciar o DB2:

```
db2start
```

Verificando o DB2

Para verificar se o DB2 está sendo executado, execute os comandos a seguir. Este procedimento supõe que o db2inst1 seja o ID do proprietário da Instância do DB2.

```
su - db2inst1
db2 create database test1
db2 connect to test1 user db2inst1 using db2instpass
db2 disconnect test1
db2 drop database test1
```

Certifique-se de que cada comando esteja sendo executado com êxito.

RQS nº 03/2005 CN
CPMI CORREIOS
Fls Nº 1532
Doc 3698

Capítulo 5. Instalando o Gerenciador do Windows

Para poder instalar o gerenciador, você deve ter concluído as etapas no Capítulo 3, "Preparando-se para a Instalação (Gerenciador do Windows)", na página 19.

Nota:

- Se você já tiver instalado o Tivoli Storage Area Network Manager e quiser salvar as informações no banco de dados antes de reinstalar o gerenciador, deverá utilizar comandos do DB2 para fazer o backup desse banco de dados. Para obter informações sobre os comandos do DB2 para fazer backup de um banco de dados, consulte *DB2 Universal Database: Referência de Comandos*. O nome padrão do banco de dados Tivoli Storage Area Network Manager é **itsanmdb**.
- O IBM Tivoli Storage Area Network Manager *não* oferece suporte para o console da Web Tivoli NetView.
- É necessário parar o Windows Terminal Services antes de instalar o gerenciador. Não é possível utilizar o Windows Terminal Services para acessar o console.
- Se você estiver instalando o gerenciador ou mais de uma máquina em um domínio do Windows, os gerenciadores de máquinas diferentes poderão terminar eventualmente compartilhando o mesmo banco de dados. Para evitar esta situação, você deve utilizar nomes de bancos de dados diferentes ou nomes de usuários diferentes do DB2 quando instalar o gerenciador em máquinas diferentes.
- O Tivoli Storage Area Network Manager também instala o Tivoli NetView 7.1.3. Se você já tiver o Tivoli NetView 7.1.1 instalado, o Tivoli Storage Area Network Manager fará upgrade dele para a versão 7.1.3. Se você tiver um release do Tivoli NetView *anterior* à versão 7.1.1, o Tivoli Storage Area Network Manager solicitará a remoção da instalação do Tivoli NetView antes de instalá-lo.
- Se a instalação falhar, resolva o problema revendo os arquivos de log. Depois inicie novamente o sistema para que a instalação parcial com falha seja eliminada antes de tentar reinstalar o gerenciador.
- O IBM Tivoli Storage Area Network Manager somente oferece suporte para grupos e IDs de usuário locais. O IBM Tivoli Storage Area Network Manager não oferece suporte para grupos e IDs de usuário de domínios.
- Se estiver instalando o produto usando um diretório e não um CD, certifique-se de que os nomes dos diretórios sejam simples (sem espaços ou caracteres hífen ou sublinhado).
- Certifique-se de ter instalado o serviço SNMP e de ter definido o nome da comunidade SNMP como **Público**. Consulte "Etapa 5: Instale o Serviço SNMP" na página 29.
- Quando instalar o IBM Tivoli Storage Area Network Manager, será criado automaticamente um banco de dados DB2. O nome padrão do banco de dados é **itsanmdb**.

Antes de instalar o gerenciador, você precisará dos IDs dos usuários e das senhas mostradas em Tabela 12 na página 60. Você pode utilizar a mesma senha para todos os IDs do usuário, autenticação do host e Tivoli NetView.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1533
Doc. 3698

© Copyright IBM Corp. 2002, 2003

Tabela 12. IDs de Usuários e Senhas Obrigatórios para a Instalação (Gerenciador Windows)

Item	Obrigatório	Suas Informações
ID do usuário e senha do administrador DB2	ID de usuário do Windows para criar o banco de dados do IBM Tivoli Storage Area Network Manager. Certifique-se de que a senha não tenha expirado ao instalar ou executar o IBM Tivoli Storage Area Network Manager. Este ID de usuário administrativo deve ser o mesmo que foi criado ou utilizado durante a instalação do DB2.	
ID do usuário e senha do DB2 para acessar o banco de dados	ID de usuário do Windows para acessar o banco de dados do IBM Tivoli Storage Area Network Manager. Se um ID de usuário não existir antes da instalação do IBM Tivoli Storage Area Network Manager, será criado durante essa instalação. Certifique-se de que a senha não tenha expirado antes de instalar ou executar o IBM Tivoli Storage Area Network Manager. Você pode alterar esta senha para "nunca expirar". Se desejar alterar a senha de ID do usuário do DB2, siga essas etapas: 1. Altere a senha no sistema operacional. 2. Altere a senha em IBM Tivoli Storage Area Network Manager (consulte o comando **srmcp ConfigService setPw** no *IBM Tivoli Storage Area Network Manager: Guia do Usuário*).	
ID do usuário e senha para o WebSphere	Deve ser um ID do usuário e uma senha existentes.	
Somente senha de autenticação do host (ID do usuário não obrigatório)	Você insere essa senha durante a instalação para permitir a comunicação de hosts gerenciados e consoles remotos com o gerenciador. Se for alterada no computador do gerenciador, também deverá ser alterada em qualquer host gerenciado ou console remoto que se comunique com esse gerenciador. É possível alterar essa senha utilizando o comando **srmcp ConfigService SetAuthenticationPw**. Para obter informações sobre esse comando, consulte a *IBM Tivoli Storage Area Network Manager: Guia do Usuário*.	

Tabela 12. IDs de Usuários e Senhas Obrigatórios para a Instalação (Gerenciador Windows) (continuação)

Item	Obrigatório	Suas Informações
Somente senha do Tivoli NetView	ID de usuário do Windows para acessar o Tivoli NetView. Se o Tivoli NetView for instalado durante a instalação do IBM Tivoli Storage Area Network Manager, o ID de usuário **netview** será criado. Esse ID de usuário é utilizado para executar o serviço NetView. Será solicitada a senha somente se o IBM Tivoli Storage Area Network Manager instalar o Tivoli NetView.	

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 1534
Doc. 3698

Instalando o Gerenciador

Siga estas instruções para instalar o gerenciador:

1. É necessário ter um ID de administrador DB2 para instalar o Tivoli Storage Area Network Manager.
2. Se você tiver o Tivoli NetView 7.1.3 instalado, certifique-se de que os seguintes aplicativos estejam encerrados:
   - Web Console
   - Web Console Security
   - MIB Loader
   - MIB Browser
   - Netmon Seed Editor
   - Tivoli Event Console Adaptor Configurator

   Além disso, certifique-se de que os Serviços de Terminal do Windows 2000 não estejam em execução.

3. Insira o CD do Tivoli Storage Area Network Manager (Manager and Remote Console) na unidade de disco de CD-ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD-ROM do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **launch.exe**. O painel Ativar é exibido. Selecione **Manager**. Clique em **Avançar** para continuar.

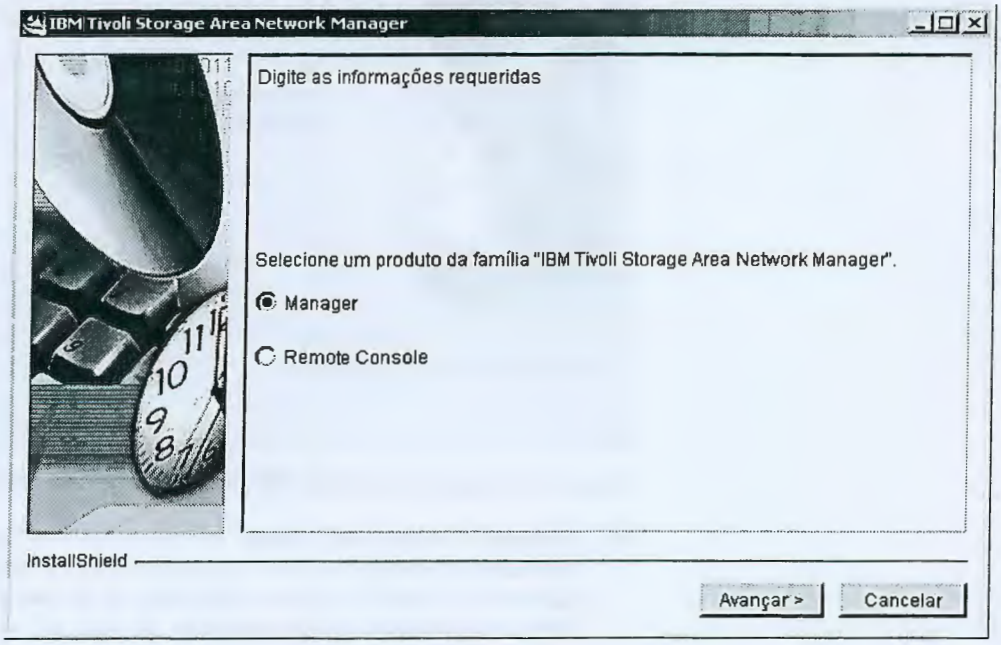


Figura 41. Painel Ativar

4. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para a instalação deste produto.

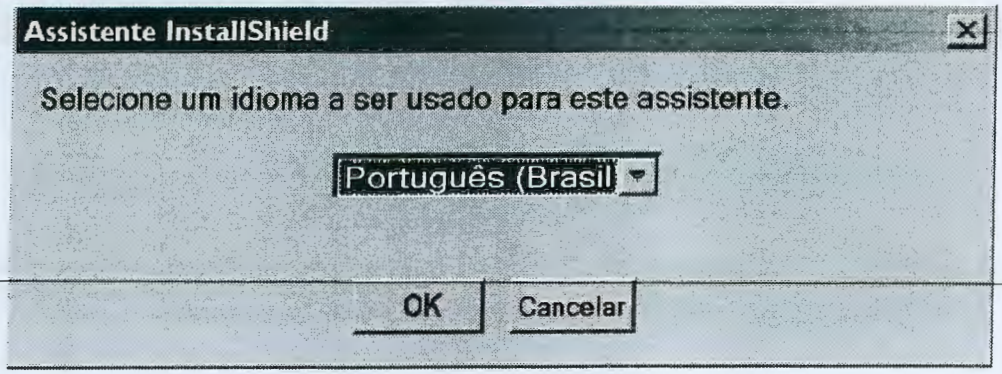


Figura 42. Painel Selecione um Idioma

ROS Nº 3[illegible] - CN
CPMI - CORREIOS
Fls. Nº 1535
Doc. 3698

10829 A.

5. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

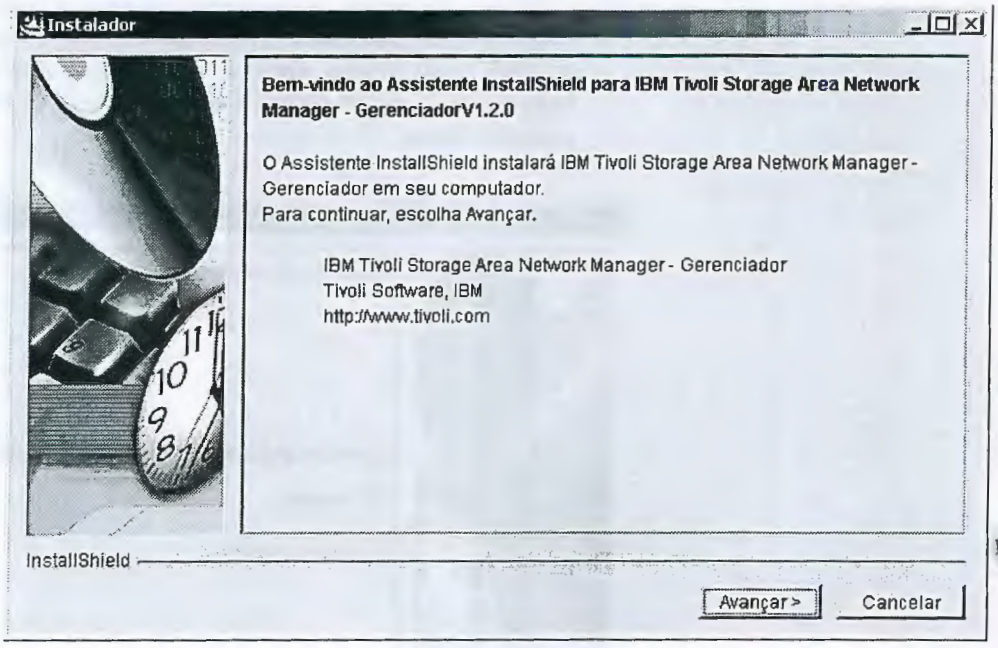


Figura 43. Painel Bem-vindo ao IBM Tivoli Storage Area Network Manager

6. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o Tivoli Storage Area Network Manager.

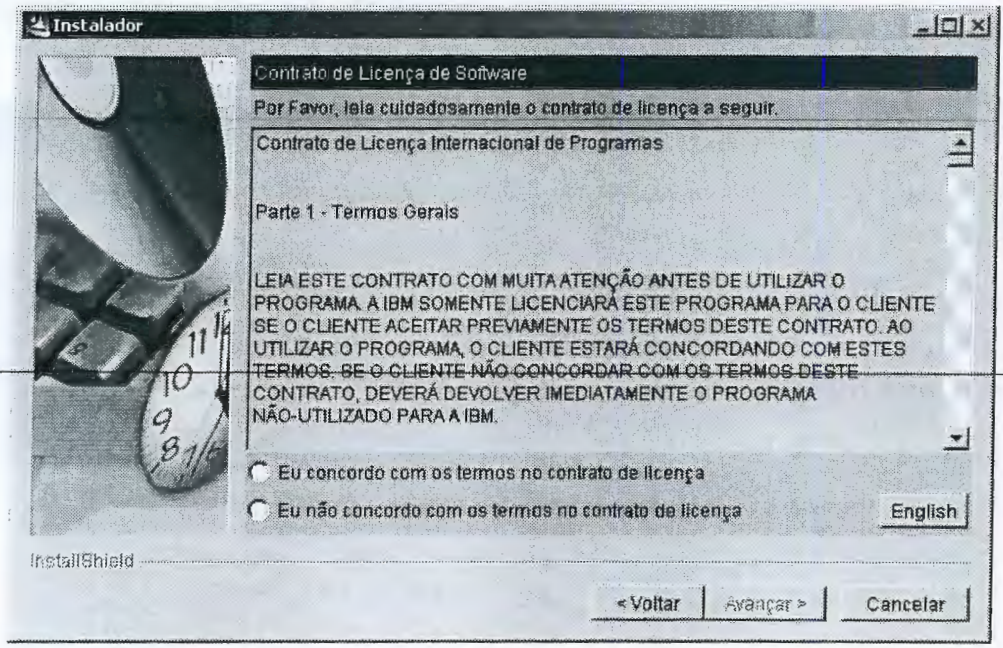


Figura 44. Painel Contrato de Licença de Software

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1536
3698
Doc.

7. O painel Informações sobre o Diretório é exibido. Insira um nome de diretório diferente ou aceite o nome de diretório padrão. O programa de instalação criará o diretório padrão se ele ainda não existir. Clique em **Avançar** para continuar.

> **Nota**
>
> - Não utilize espaços ou hifens em nomes de diretório.
> - Se você estiver instalando o gerenciador do AIX, o caminho do diretório será diferente. Por exemplo, o caminho do diretório pode ser: `/tivoli/itsanm/manager`.

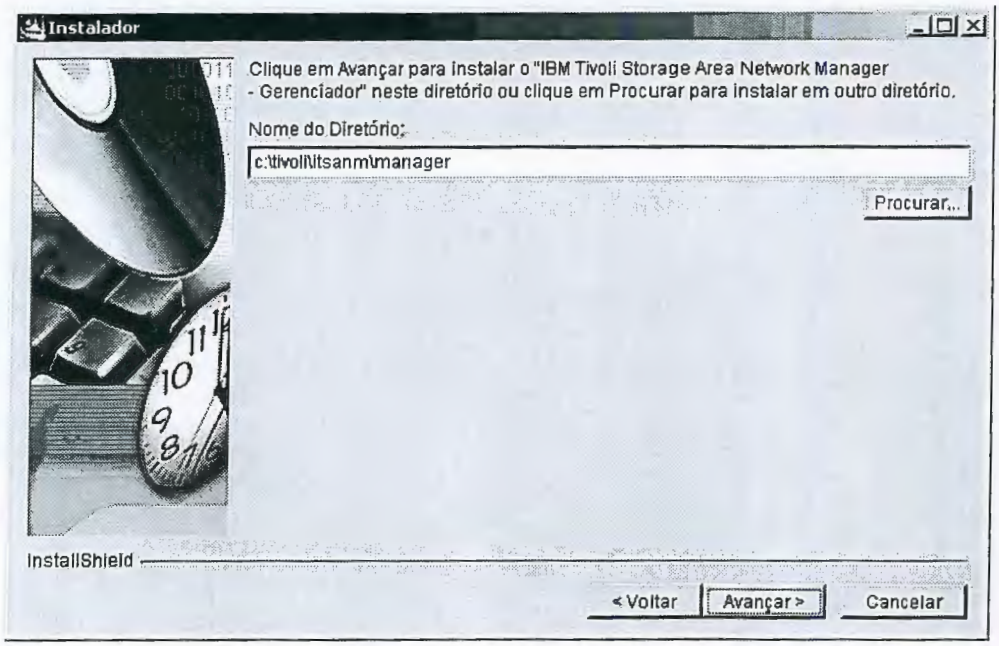


Figura 45. Painel Informações sobre o Diretório

8. O painel Número de Porta é exibido. Ele consiste em uma faixa de sete números de porta a serem utilizados pelo Tivoli Storage Area Network Manager. O primeiro número de porta que você especificar será considerado o *número de porta base*. Somente é necessário inserir esse número de porta base. O número de porta base e os 6 números seguintes serão reservados para uso por parte do Tivoli Storage Area Network Manager. Por exemplo, se você especificar o número de porta 9550, o Tivoli Storage Area Network Manager utilizará os números de porta entre 9550 e 9556.

   Certifique-se de que os números de porta que você utilizar não sejam utilizados por outros aplicativos. Para determinar quais números de porta estão sendo utilizados em um computador específico, digite um dos comandos a seguir em um prompt de comandos:

   ```
   netstat -a
   netstat -an
   ```

   Os números de porta em uso no sistema são listados na coluna Endereço Local da saída. Esse campo possui o formato *host:porta*.

   Insira o número de porta base e clique em **Avançar** para continuar.

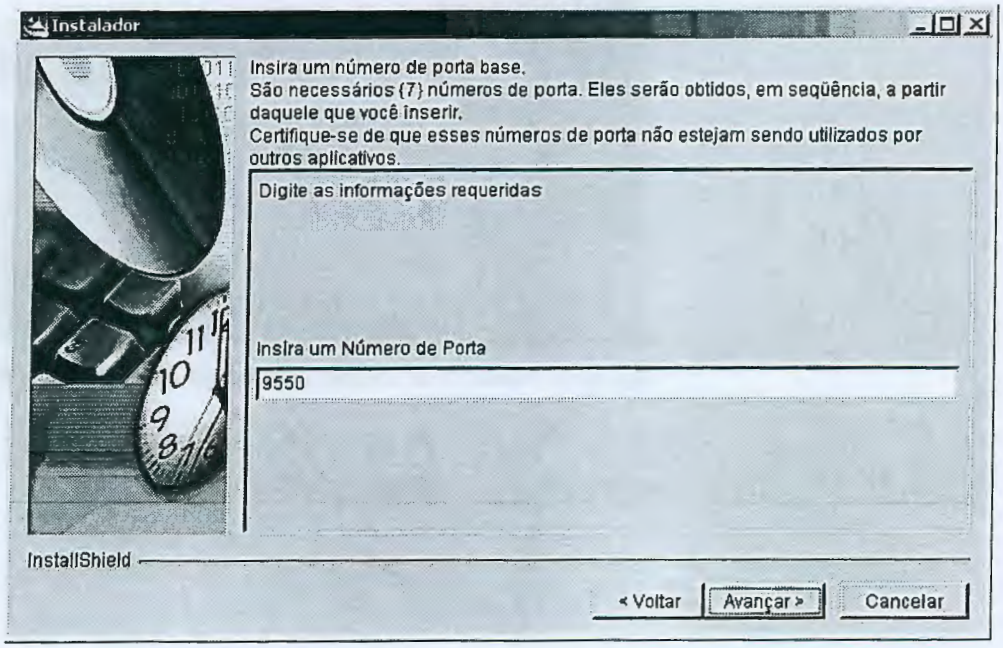


Figura 46. Painel Número de Porta

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1536
Doc. 3698

9. O painel ID do Usuário e Senha do Administrador DB2 é exibido. Para obter informações sobre esse ID de usuário do administrador DB2 do Windows, consulte a Tabela 12 na página 60. Insira o ID do administrador DB2 e insira a senha duas vezes. Certifique-se de que a senha não tenha expirado. Clique em **Avançar** para continuar.

   Nota: Se estiver instalando o gerenciador do AIX, este ID do usuário e esta senha são para o proprietário da instância do DB2 (por exemplo, db2inst1).

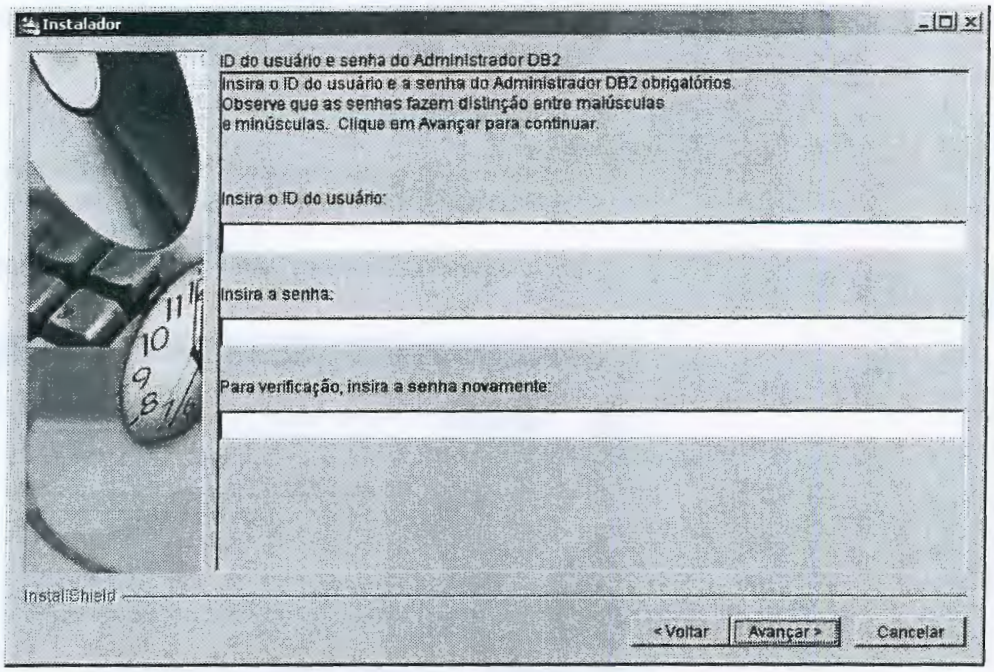


Figura 47. Painel ID do Usuário e Senha do Administrador DB2

10. O painel ID do Usuário e Senha DB2 é exibido. Para obter informações sobre esse ID de usuário do Windows, consulte a Tabela 12 na página 60. Insira um ID do usuário DB2 e uma senha duas vezes.

    O nome padrão do banco de dados é **itsanmdb**. Se esse não for o seu banco de dados, insira o nome correto do banco de dados. O nome do banco de dados deve conter no máximo oito caracteres. Clique em **Avançar** para continuar.

    Nota: Se você estiver utilizando um ID de usuário e uma senha existentes, o programa de instalação não validará essa senha. Certifique-se de que o ID do usuário e a senha sejam válidos. Antes de continuar o programa de instalação, certifique-se também de que a senha não tenha expirado.

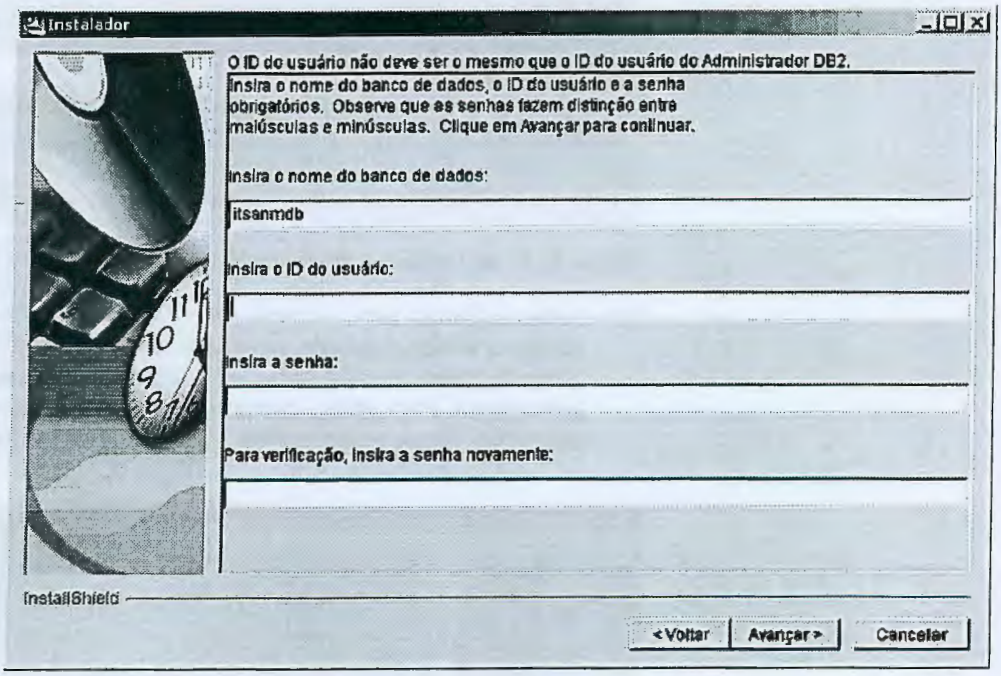


Figura 48. Painel ID do Usuário e Senha DB2

11. O ID do Usuário e a Senha para o painel WebSphere é exibido. Insira o ID de usuário e a senha duas vezes.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1538
Doc. 3698

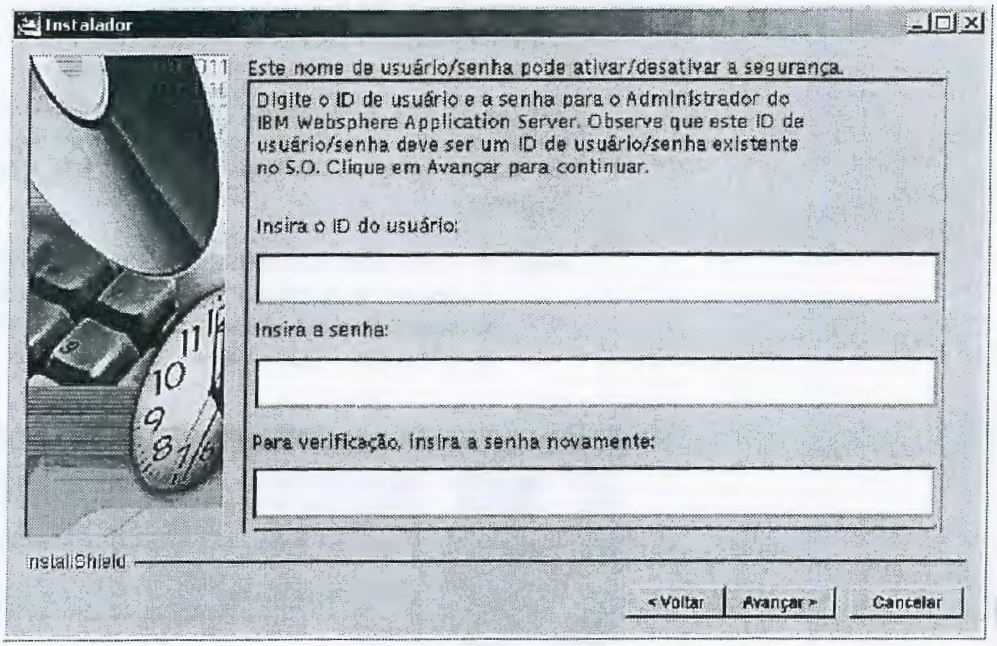


Figura 49. ID do Usuário e Senha para o Painel WebSphere

12. O painel Senha para Autenticação do Host é exibido. É possível inserir qualquer senha desejada, mas essa mesma senha deve ser utilizada para todos os hosts gerenciados e consoles remotos que se comunicam com esse gerenciador. Para obter informações sobre essa senha, consulte a Tabela 12 na página 60. Insira a senha duas vezes. Clique em **Avançar** para continuar.

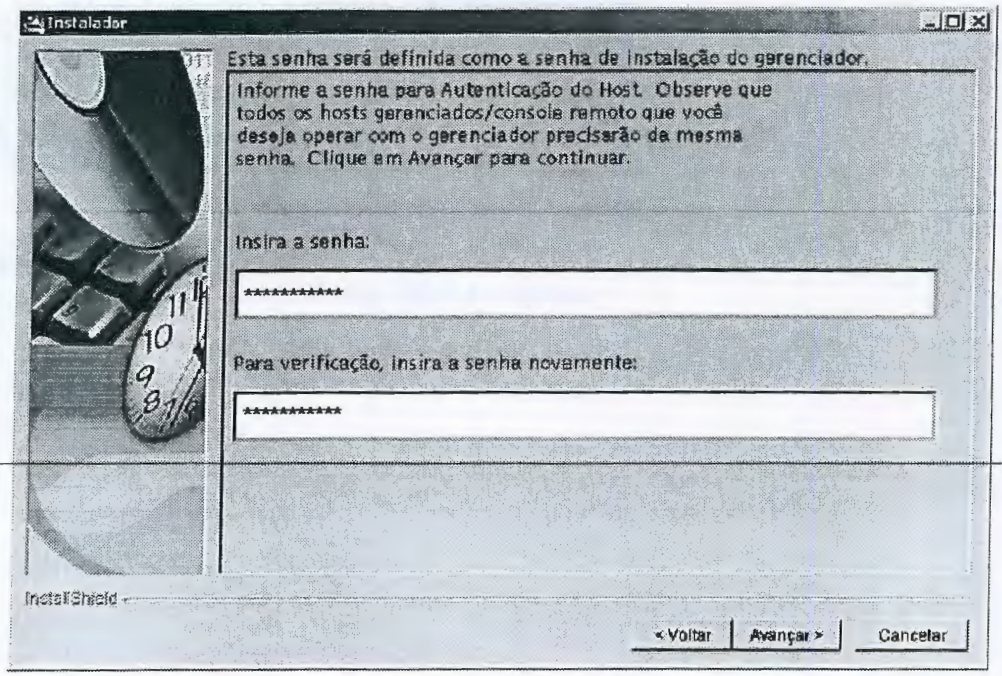


Figura 50. Painel Senha para Autenticação do Host

13. O painel Nome da Unidade do Tivoli NetView é exibido. Insira o nome da unidade na qual você deseja instalar o Tivoli NetView. Clique em **Avançar** para continuar.

Nota:

- Se você tiver o Tivoli NetView 7.1.3 instalado, esse painel não será exibido.
- Se você estiver instalando o gerenciador do AIX, esse painel não será exibido.

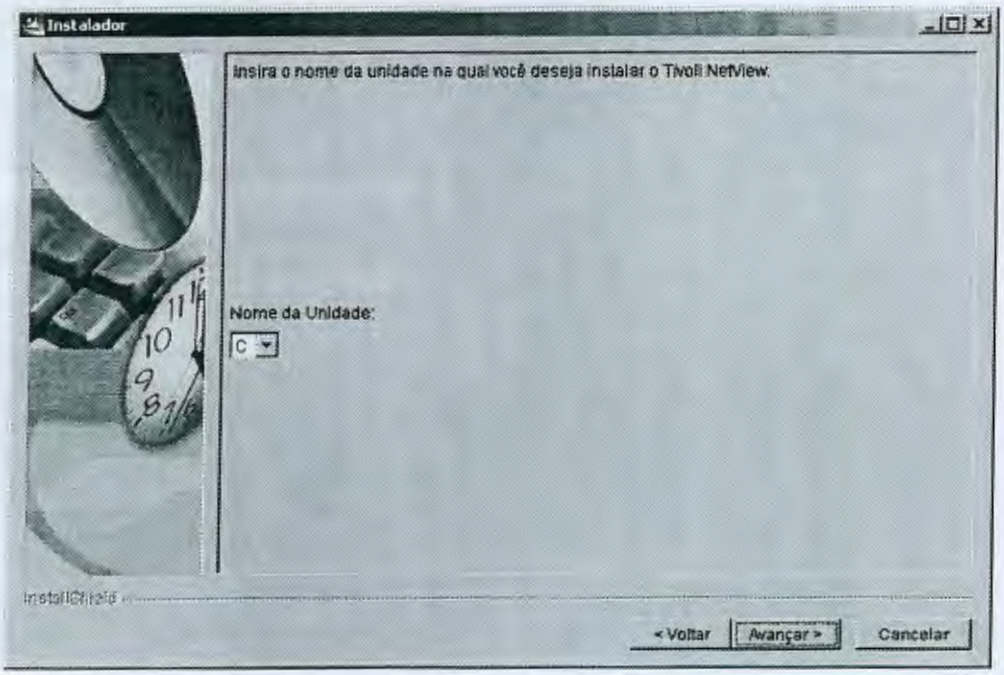


Figura 51. Painel Nome da Unidade do Tivoli NetView

RQS nº 03/2005 - CN
CPMI
Fls. Nº 1539
Doc. 3698

14. O painel Senha do Tivoli NetView é exibido. Para obter informações sobre o ID do usuário e a senha, consulte a Tabela 12 na página 60. Insira a senha duas vezes. Clique em **Avançar** para continuar.

Nota:

- Se você tiver o Tivoli NetView 7.1.3 instalado, esse painel não será exibido.
- Se você estiver instalando o gerenciador do AIX, esse painel não será exibido.

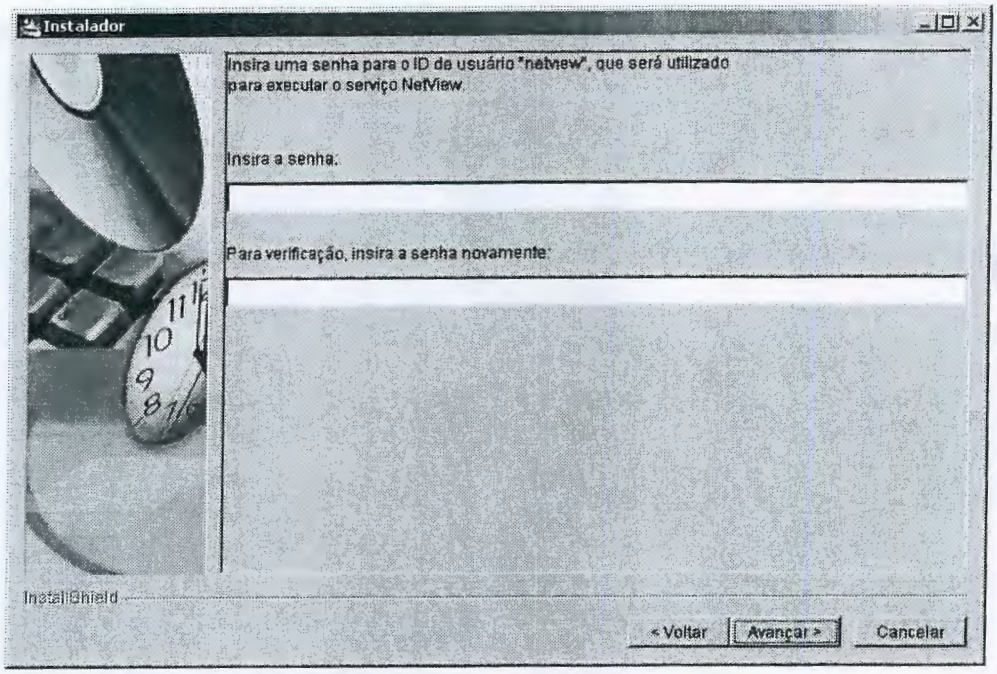


Figura 52. Painel Senha do Tivoli NetView

15. O painel Instalação do Tivoli Storage Area Network Manager é exibido. Clique em **Avançar** para continuar.

Nota: Se você estiver instalando o gerenciador do AIX, o caminho do diretório será diferente. Por exemplo, o caminho do diretório pode ser: `/tivoli/itsanm/manager`.

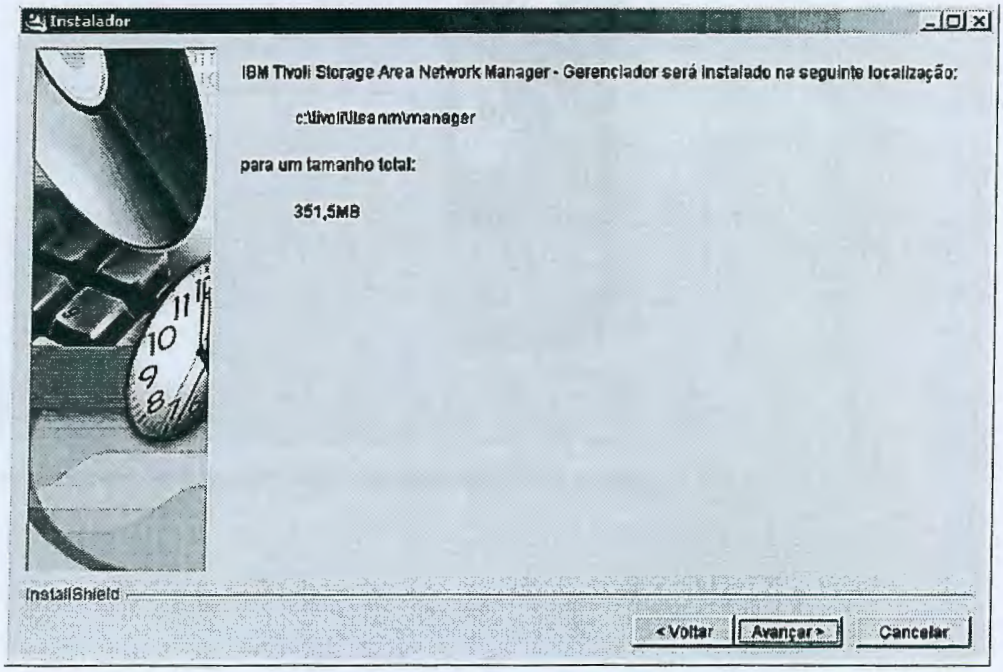


Figura 53. Painel Instalação do Tivoli Storage Area Network Manager

16. O painel Status é exibido. Esse procedimento pode levar aproximadamente de 15 a 20 minutos para ser concluído.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1540
3698
Doc.

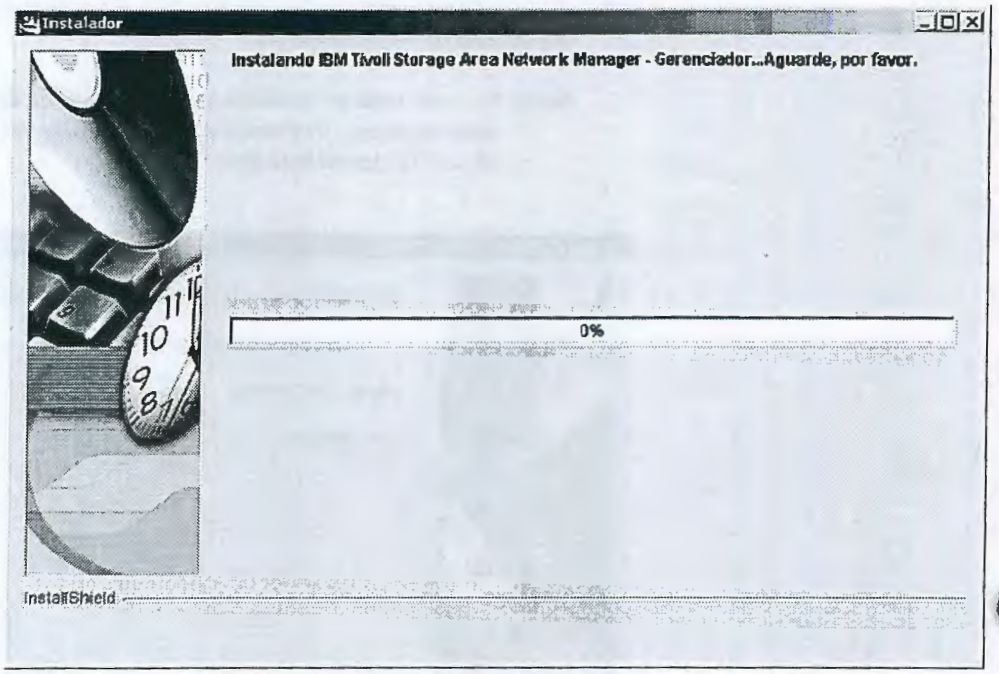


Figura 54. Painel Status do Tivoli Storage Area Network Manager

17. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido.

    Se a versão correta do Tivoli NetView tiver sido instalada antes da instalação do gerenciador, o botão **Concluir** será exibido. (O Tivoli NetView não será instalado com o gerenciador.) Você não verá o painel seguinte que solicita a reinicialização do sistema.

    Se o Tivoli NetView não tiver sido instalado anteriormente e for instalado com essa instalação do gerenciador, o painel seguinte será exibido. Esse painel solicita a reinicialização do sistema.

    Clique em **Concluir** ou **Avançar** para continuar.

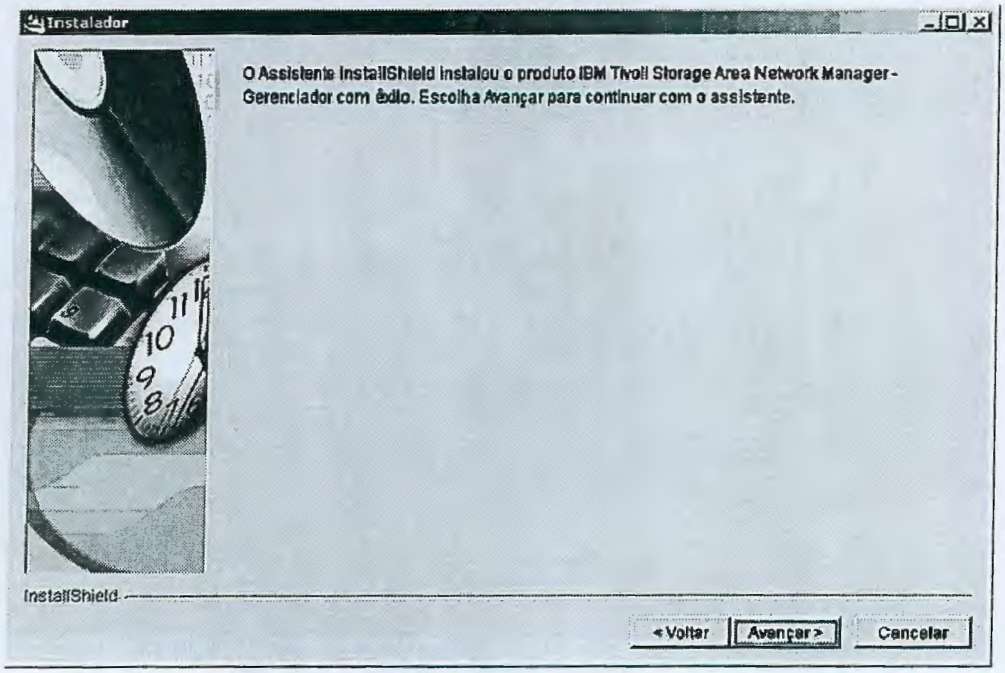


Figura 55. Painel Instalado com Êxito

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1541
3698
Doc.

18. O painel Instalação Concluída é exibido. Para iniciar o computador novamente, clique em **Sim, reinicialize meu sistema.** Clique em **Concluir** para concluir a instalação.

    Nota:

    - Se você tiver o Tivoli NetView 7.1.3 instalado, esse painel não será exibido.
    - Se você estiver instalando o gerenciador do AIX, esse painel não será exibido.

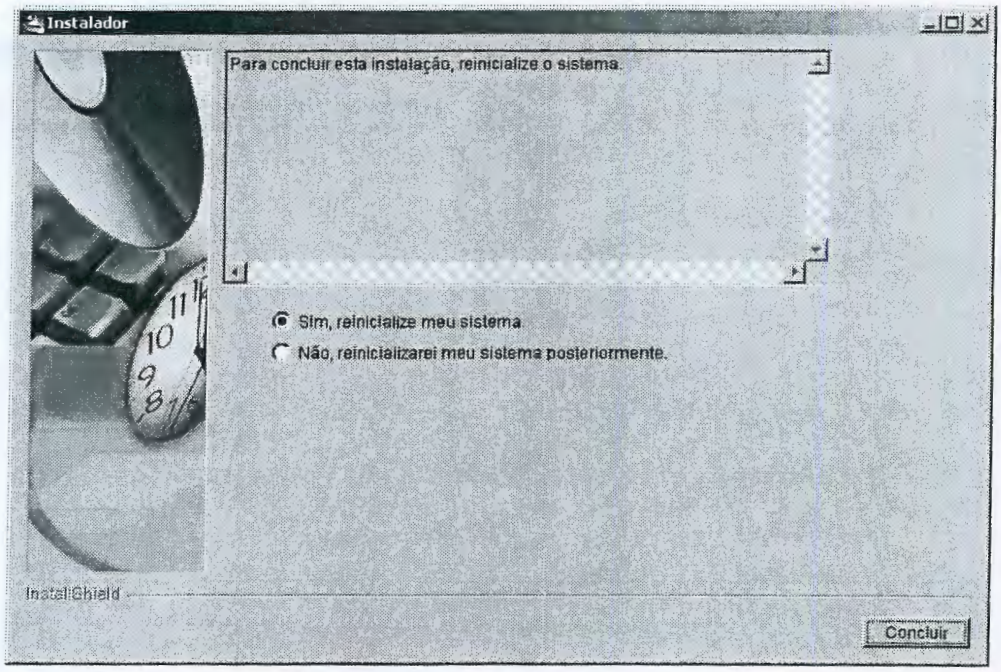


Figura 56. Painel Instalação Concluída

19. Depois de iniciar novamente o sistema, o serviço do Tivoli Storage Area Network Manager será automaticamente iniciado.
20. É recomendado configurar seu banco de dados DB2 após instalar o IBM Tivoli Storage Area Network Manager. Consulte "Configurando o Banco de Dados DB2" na página 201.

Iniciando e Parando o Gerenciador

Para iniciar o gerenciador, siga estas etapas:

1. Na barra de ferramentas, clique no seguinte:

   ```
   Iniciar -> Configurações -> Painel de Controle ->
   Ferramentas Administrativas -> Serviços
   ```

2. No painel Serviços, localize e realce **IBM WebSphere Application Server V5 – ITSANM – Manager**.
3. Dê um clique com o botão direito do mouse em **IBM WebSphere Application Server V5 – ITSANM–Manager**.
4. Dê um clique em **Iniciar**.

Para parar o gerenciador, siga estas etapas:

1. Na barra de ferramentas, clique no seguinte:

   `Iniciar → Configurações → Painel de Controle → Ferramentas Administrativas → Serviços`
2. No painel Serviços, localize e realce **IBM WebSphere Application Server V5 – ITSANM – Manager**.
3. Dê um clique com o botão direito do mouse em **IBM WebSphere Application Server V5 – ITSANM–Manager**.
4. Clique em **Parar**.

Verificando os Arquivos de Log

Depois de instalar o gerenciador, verifique este log para determinar se ocorreram erros (utilizando o diretório padrão):

`c:\tivoli\itsanm\manager\mgrlog.txt`

Se você encontrar erros de instalação, existem outros logs que podem ser verificados para determinar o local em que os problemas ocorreram. Os logs encontram-se neste diretório:

`c:\tivoli\itsanm\manager\log\install\`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1542
Nº - 3698
Doc.

10216
1543

Capítulo 6. Instalando o Gerenciador do AIX

Para poder instalar o gerenciador, você deve ter concluído as etapas no Capítulo 4, "Preparando-se para a Instalação (Gerenciador do AIX)", na página 35.

Nota:

- Se você já tiver instalado o Tivoli Storage Area Network Manager e quiser salvar as informações no banco de dados antes de reinstalar o gerenciador, deverá utilizar comandos do DB2 para fazer o backup desse banco de dados. Para obter informações sobre os comandos do DB2 para fazer backup de um banco de dados, consulte *DB2 Universal Database: Referência de Comandos*. O nome padrão do banco de dados Tivoli Storage Area Network Manager é **itsanmdb**.
- O IBM Tivoli Storage Area Network Manager *não* oferece suporte para o console da Web Tivoli NetView.
- O Tivoli NetView não está instalado e não é suportado no gerenciador do AIX. Se desejar ver a exibição da GUI do IBM Tivoli Storage Area Network Manager, instale o console remoto no Windows 2000 ou no Windows XP.
- Se a instalação falhar, resolva o problema revendo os arquivos de log. Depois reinicialize o sistema para limpar a instalação parcial antes de tentar reinstalar o gerenciador.
- O IBM Tivoli Storage Area Network Manager somente oferece suporte para grupos e IDs de usuário locais. O IBM Tivoli Storage Area Network Manager não oferece suporte para grupos e IDs de usuário de domínios.
- Se estiver instalando o produto de um diretório e não do CD, certifique-se de que os nomes de diretório sejam nomes simples (sem espaços, nem caracteres hífen ou sublinhado).
- Quando instalar o IBM Tivoli Storage Area Network Manager, será criado automaticamente um banco de dados DB2. O nome padrão do banco de dados é **itsanmdb**.

Antes de instalar o gerenciador, você precisará dos IDs dos usuários e das senhas mostradas em Tabela 13. Você pode utilizar a mesma senha para todos os IDs do usuário e autenticação do host.

Tabela 13. IDs de Usuários e Senhas Obrigatórios para a Instalação (Gerenciador do AIX)

Item	Obrigatório	Suas Informações
ID de proprietário e senha da instância de DB2	Este é um ID do usuário para criar o banco de dados do IBM Tivoli Storage Area Network Manager. Consulte 6 na página 49. Certifique-se de que a senha não tenha expirado ao instalar ou executar o IBM Tivoli Storage Area Network Manager.	

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1543
Doc. 3698

Tabela 13. IDs de Usuários e Senhas Obrigatórios para a Instalação (Gerenciador do AIX) (continuação)

Item	Obrigatório	Suas Informações
ID do usuário e senha do DB2 para acessar o banco de dados	ID de usuário do AIX para acessar o banco de dados do IBM Tivoli Storage Area Network Manager. Certifique-se de que a senha não tenha expirado antes de instalar ou executar o IBM Tivoli Storage Area Network Manager. Se desejar alterar a senha de ID do usuário, siga essas etapas: 1. Altere a senha no sistema operacional. 2. Altere a senha no IBM Tivoli Storage Area Network Manager (consulte o comando **srmcp ConfigService setPw** no *IBM Tivoli Storage Area Network Manager: Guia do Usuário*).	
ID do usuário e senha para o WebSphere	Deve ser um ID do usuário e uma senha existentes.	
Somente senha de autenticação do host (ID do usuário não obrigatório)	Você insere essa senha durante a instalação para permitir a comunicação de hosts gerenciados e consoles remotos com o gerenciador. Se for alterada no computador do gerenciador, também deverá ser alterada em qualquer host gerenciado ou console remoto que se comunique com esse gerenciador. É possível alterar essa senha utilizando o comando **srmcp ConfigService SetAuthenticationPw**. Para obter informações sobre esse comando, consulte a *IBM Tivoli Storage Area Network Manager: Guia do Usuário*.	

Instalando o Gerenciador do AIX

Estas instruções utilizam painéis semelhantes à instalação do gerenciador no Windows e referem-se a esses painéis.

Siga estas instruções para instalar o gerenciador:

1. É necessário ter um ID de administrador DB2 para instalar o Tivoli Storage Area Network Manager.
2. Utilize esses comandos para criar o diretório e determine o diretório de montagem. O comando também executa o script de instalação. O script de instalação está localizado no diretório **manager**. Execute estes comandos:

```
mkdir /cdrom
mount -v'cdrfs' -r'' /dev/cd0 /cdrom
cd /cdrom/manager
./setup.aix
```

Observe que a opção –r é acompanhada de duas aspas.

10214
A

3. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para a instalação deste produto. Consulte a etapa 4 na página 63.
4. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.
5. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o Tivoli Storage Area Network Manager.
6. O painel Informações sobre o Diretório é exibido. Insira um nome de diretório diferente ou aceite o nome de diretório padrão. O programa de instalação criará o diretório padrão se ele ainda não existir. Clique em **Avançar** para continuar.

   Nota: Não utilize espaços ou hifens em nomes de diretório.
7. O painel Número de Porta é exibido. Ele consiste em uma faixa de sete números de porta a serem utilizados pelo Tivoli Storage Area Network Manager. O primeiro número de porta que você especificar será considerado o *número de porta base*. Somente é necessário inserir esse número de porta base. O número de porta base e os 6 números seguintes serão reservados para uso por parte do Tivoli Storage Area Network Manager. Por exemplo, se você especificar o número de porta 9550, o Tivoli Storage Area Network Manager utilizará os números de porta entre 9550 e 9556.

   Certifique-se de que os números de porta que você utilizar não sejam utilizados por outros aplicativos.

   Insira o número de porta base e clique em **Avançar** para continuar.
8. O painel ID do Usuário e Senha do Administrador DB2 é exibido. Este ID do usuário e esta senha são do proprietário da instância do DB2 (por exemplo, db2inst1). Consulte Tabela 13 na página 79. Digite o ID do proprietário da instância do DB2 e digite a senha duas vezes. Certifique-se de que a senha não tenha expirado. Clique em **Avançar** para continuar.
9. O painel ID do Usuário e Senha DB2 é exibido. Para obter informações sobre esse ID de usuário, consulte a Tabela 13 na página 79. Insira um ID do usuário DB2 e uma senha duas vezes.

   O nome padrão do banco de dados é **itsanmdb**. Se esse não for o seu banco de dados, insira o nome correto do banco de dados. O nome do banco de dados deve conter no máximo oito caracteres. Clique em **Avançar** para continuar.

   Nota: Se você estiver utilizando um ID de usuário e uma senha existentes, o programa de instalação não validará essa senha. Certifique-se de que o ID do usuário e a senha sejam válidos. Antes de continuar o programa de instalação, certifique-se também de que a senha não tenha expirado.
10. O ID do Usuário e a Senha para o painel WebSphere é exibido. Insira o ID de usuário e a senha duas vezes.
11. O painel Senha para Autenticação do Host é exibido. É possível inserir qualquer senha desejada, mas essa mesma senha deve ser utilizada para todos os hosts gerenciados e consoles remotos que se comunicam com esse gerenciador. Para obter informações sobre essa senha, consulte a Tabela 13 na página 79. Insira a senha duas vezes. Clique em **Avançar** para continuar.
12. O painel Instalação do Tivoli Storage Area Network Manager é exibido. Clique em **Avançar** para continuar.

CPMI CORREIOS
Fls - Nº 1544
Nº Doc. 3698

13. O painel Status do Tivoli Storage Area Network Manager é exibido. Esse procedimento pode levar aproximadamente de 15 a 20 minutos para ser concluído. Você verá outras janelas de prompt de comandos se abrindo e fechando conforme a instalação continua.
14. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido.

    Clique em **Concluir** para sair do assistente.
15. É recomendado configurar o banco de dados DB2 após instalar o IBM Tivoli Storage Area Network Manager. Consulte "Configurando o Banco de Dados DB2" na página 201.

Iniciando e Parando o Gerenciador

Para iniciar o gerenciador no AIX, vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

```
/tivoli/itsanm/manager/bin/aix/startSANM.sh
```

Para parar o gerenciador no AIX, vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

```
/tivoli/itsanm/manager/bin/aix/stopSANM.sh
```

Verificando os Arquivos de Log

Depois de instalar o gerenciador, verifique este log para determinar se ocorreram erros (utilizando o diretório padrão):

```
/tivoli/itsanm/manager/mgrlog.txt
```

Se você encontrar erros de instalação, existem outros logs que podem ser verificados para determinar o local em que os problemas ocorreram. Os logs estão neste diretório:

```
/tivoli/itsanm/manager/log/install/
```

Capítulo 7. Instalando o Agente no Host Gerenciado

Importante

Antes de instalar o Tivoli Storage Area Network Manager, certifique-se que a SAN esteja operacional. Verifique o seguinte:

- Você deve ter instalado as placas HBA (adaptador de barramento de host) apropriadas e drivers de dispositivo (por exemplo, o HBA QLogic e drivers de dispositivo). Para EDFI, a API HBA comum da fase 2 deve ser instalada no host gerenciado. Isto é obrigatório para reunir estatísticas de portas. Para obter uma lista de compatibilidade de dispositivos, consulte o seguinte endereço da Web:

  `http://www-3.ibm.com/software/sysmgmt/products/support/`

  Selecione IBM Tivoli Storage Area Network Manager na lista drop down.
- Certifique-se de que o pacote de driver de dispositivo para o HBA possua suporte instalado para a API HBA comum ou que você tenha executado um programa de instalação separado para esse pacote. Em caso de dúvidas, entre em contato com o fabricante do HBA.

Atenção:

Recomendamos que você não instale os agentes do Tivoli Storage Area Network Manager em servidores que se comunicam com dispositivos de mídia removível. Sempre que um processo de discovery é executado, os agentes enviam comandos SCSI aos dispositivos para identificar o tipo desses dispositivos. Se o destino for um dispositivo de mídia removível que não consegue manipular o enfileiramento de comandos, poderá haver uma falha de comando de leitura ou gravação de fita extensa.

Nota:

- Para poder instalar o agente do Tivoli Storage Area Network Manager, é necessário ter um ID do usuário Windows com autoridade administrativa ou um ID do usuário UNIX com autoridade raiz. Também é necessário ter as informações descritas na Tabela 8 na página 21.
- Você deve ter 150 MB de espaço em disco temporário para instalar o agente.
- Para alterar o número de porta para um host gerenciado, você deve remover a instalação do agente e, em seguida, reinstalá-lo. O gerenciador considerará o host gerenciado com o número de porta alterado como um novo host gerenciado.

Instalando o Agente do IBM Tivoli Storage Area Network Manager no Windows 2000 ou NT

Você deve ter autoridade de administrador para instalar o agente. Siga estas instruções para instalar o agente do Tivoli Storage Area Network Manager:

1. Verifique se o sistema está utilizando um nome de host completo. Consulte "Verificando Nomes de Host Completos" na página 204

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1545
Doc: 3698

2. Somente para Windows NT: o programa msi da Microsoft deve estar instalado. Se esse programa não estiver instalado, visite o Web site a seguir:
   `http://www.microsoft.com/downloads/release.asp?releaseid=32832&NewList=1`

   Instale o programa msi da Microsoft a partir desse Web site antes de instalar o agente do IBM Tivoli Storage Area Network Manager.
3. Insira o CD Tivoli Storage Area Network Manager Agents na unidade de disco de CD-ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD-ROM do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **setup.exe**.
4. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para a instalação deste produto.

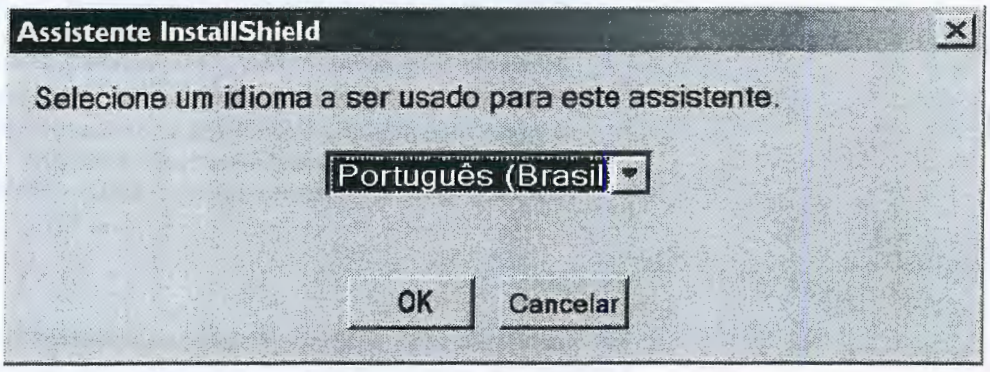


Figura 57. Painel Selecione um Idioma

5. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

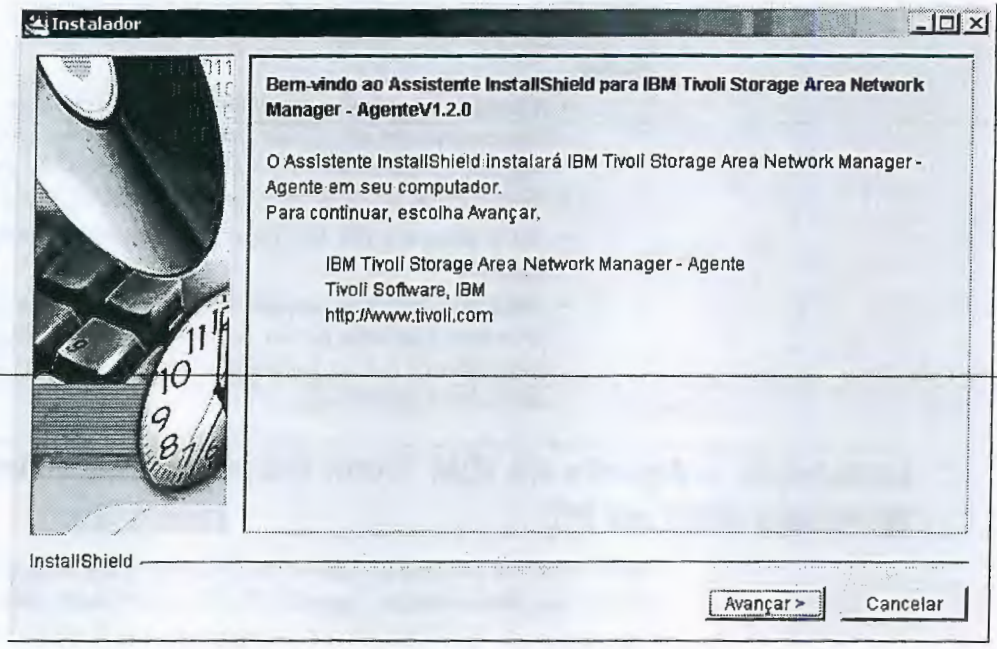


Figura 58. Painel Bem-vindo ao Tivoli Storage Area Network Manager

RQS nº 03/2005 - CN
Fls. Nº 1546
Doc. 3698

6. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o agente do Tivoli Storage Area Network Manager.

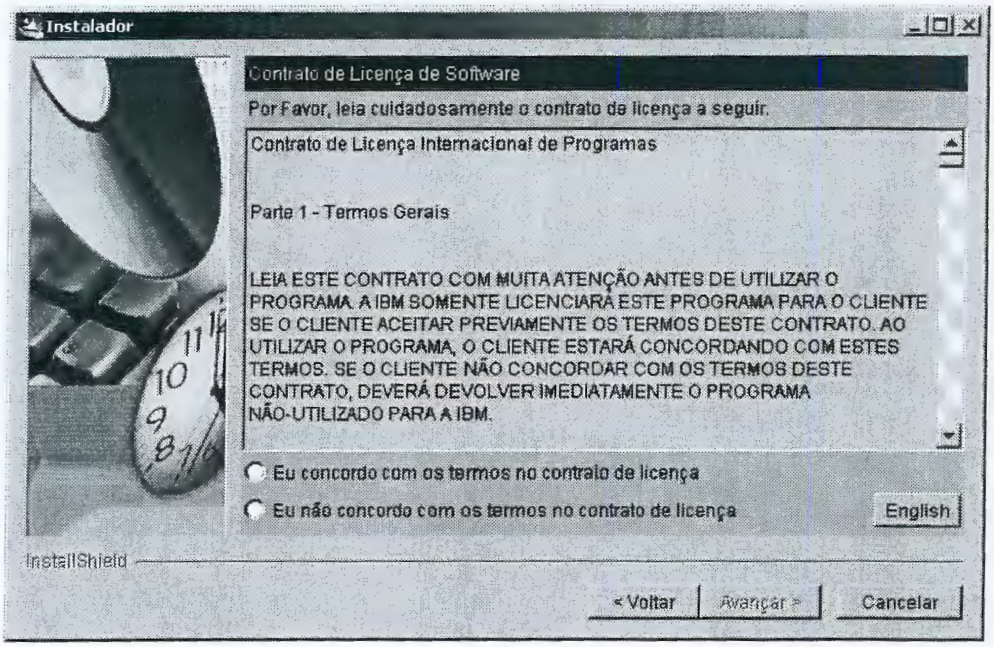


Figura 59. Painel Contrato de Licença

7. O painel Informações sobre o Diretório é exibido. Insira um nome de diretório diferente ou aceite o nome de diretório padrão. Insira um caminho absoluto para o destino, por exemplo, no Windows, `c:\tivoli\itsanm\agent`. Clique em **Avançar** para continuar.

   Nota:

   - *Não* utilize espaços ou hifens em nomes de diretório.
   - Esse painel terá um caminho de diretório diferente para a instalação no UNIX, por exemplo,

     `/tivoli/itsanm/agent`

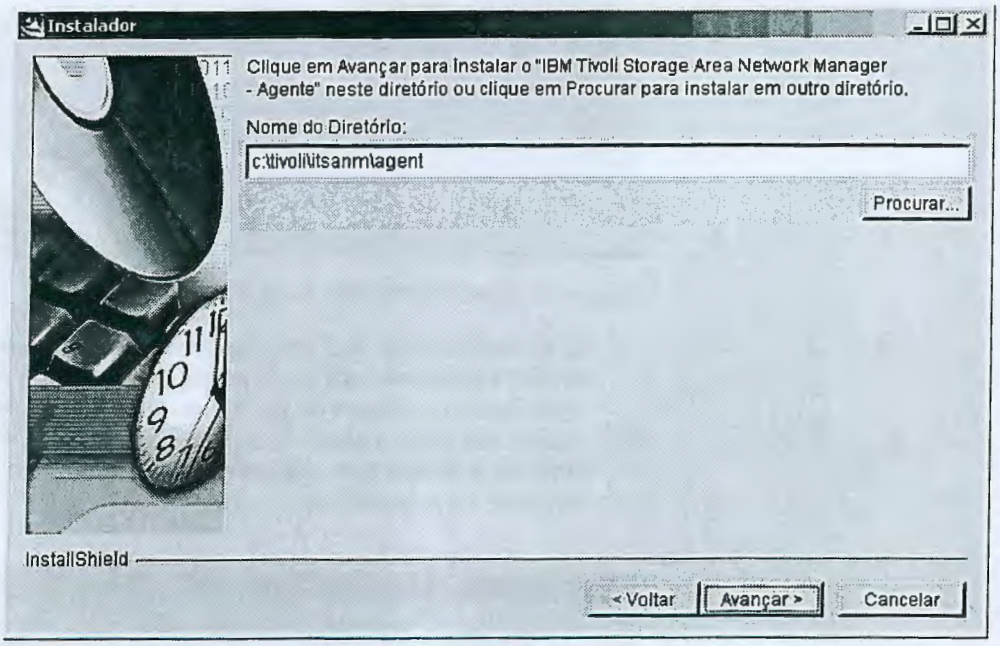


Figura 60. Painel Informações sobre o Diretório

8. O painel Informações sobre o Gerenciador é exibido. Insira um nome de host completo e um número de porta base para o Tivoli Storage Area Network Manager. O número de porta base é o primeiro número de porta especificado na etapa 8 na página 67. Clique em **Avançar** para continuar.

RQS nº 03/2005 - CN
CPMI - CORREIOS
FLS. Nº 1547
Doc. 3698

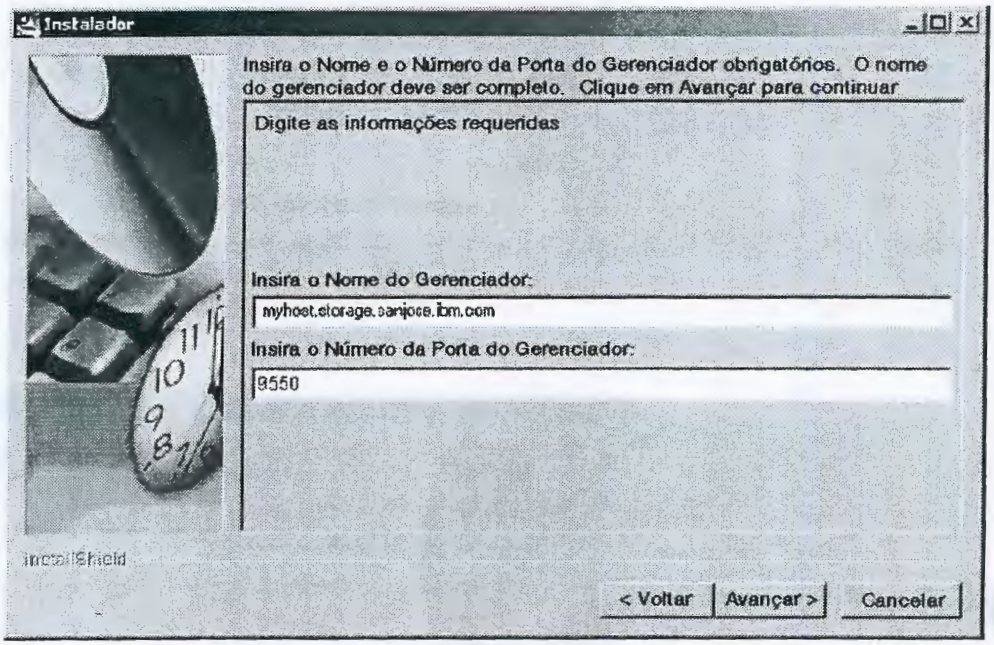


Figura 61. Painel Informações sobre o Gerenciador

9. O painel Número de Porta é exibido. Esse número de porta consiste em uma faixa de quatro números de porta. O número de porta inicial inserido é considerado o *número de porta base*. Você precisa inserir apenas o número de porta base nesse painel. Para obter informações sobre números de porta, consulte a Tabela 8 na página 21. Insira o número de porta base. Clique em **Avançar** para continuar.

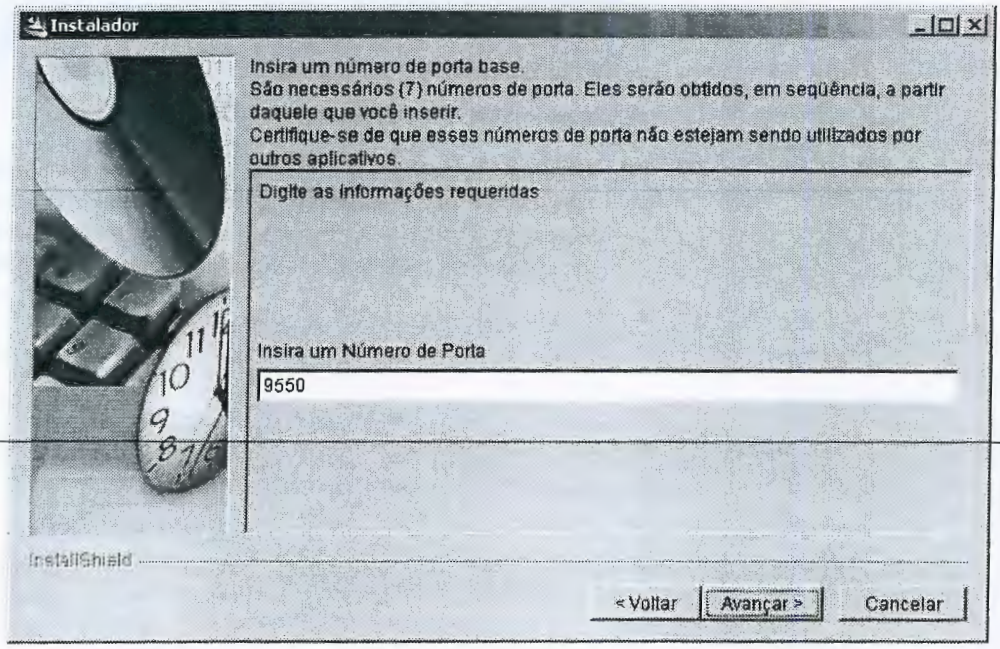


Figura 62. Painel Número de Porta

10. O painel Senha para Autenticação do Host é exibido. Essa senha deve ser a mesma senha do gerenciador com o qual este host gerenciado se comunica. Para obter informações sobre essa senha, consulte a Tabela 12 na página 60. Insira a senha duas vezes. Clique em **Avançar** para continuar.

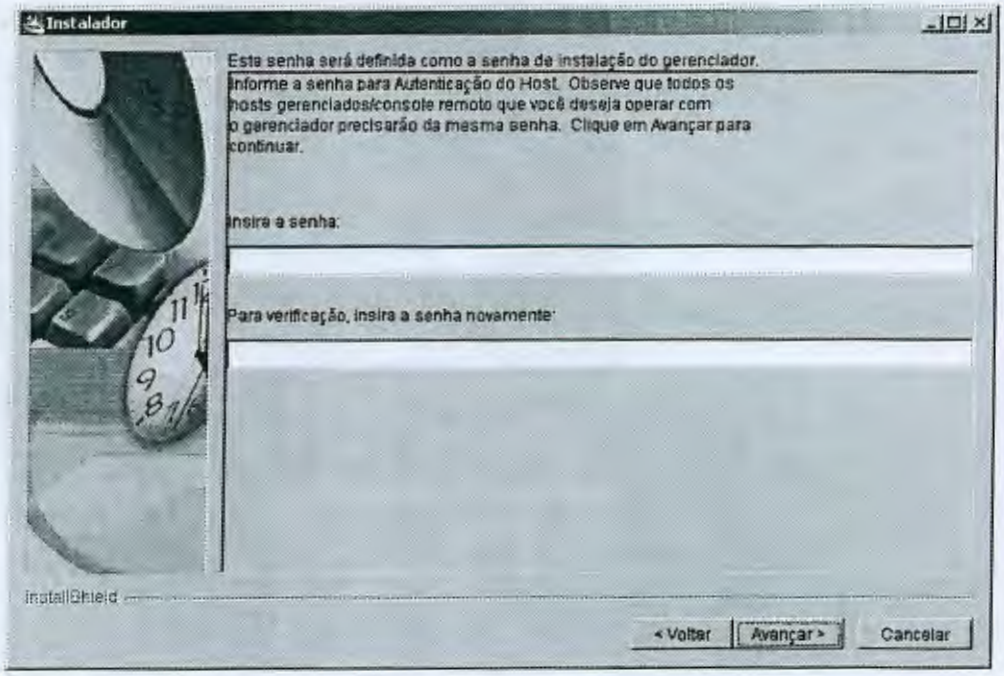


Figura 63. Painel Senha para Autenticação do Host

11. O painel Confirmação é exibido. Clique em **Avançar** para concluir.

Nota: Nos sistemas UNIX, o caminho do diretório é `/tivoli/itsanm/agent`.

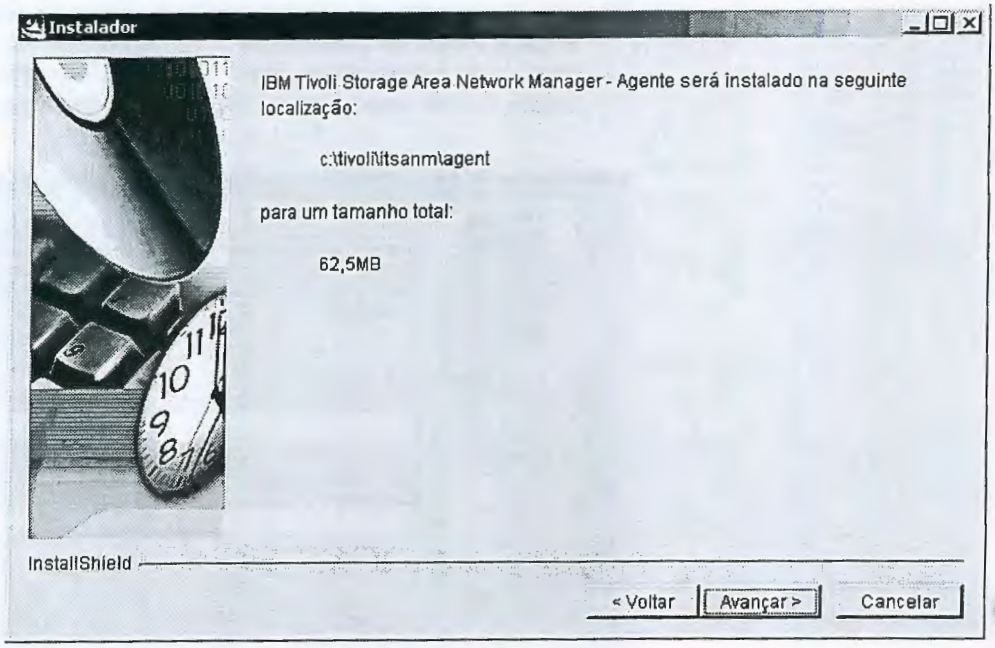


Figura 64. Painel Confirmação

12. O painel Status é exibido.

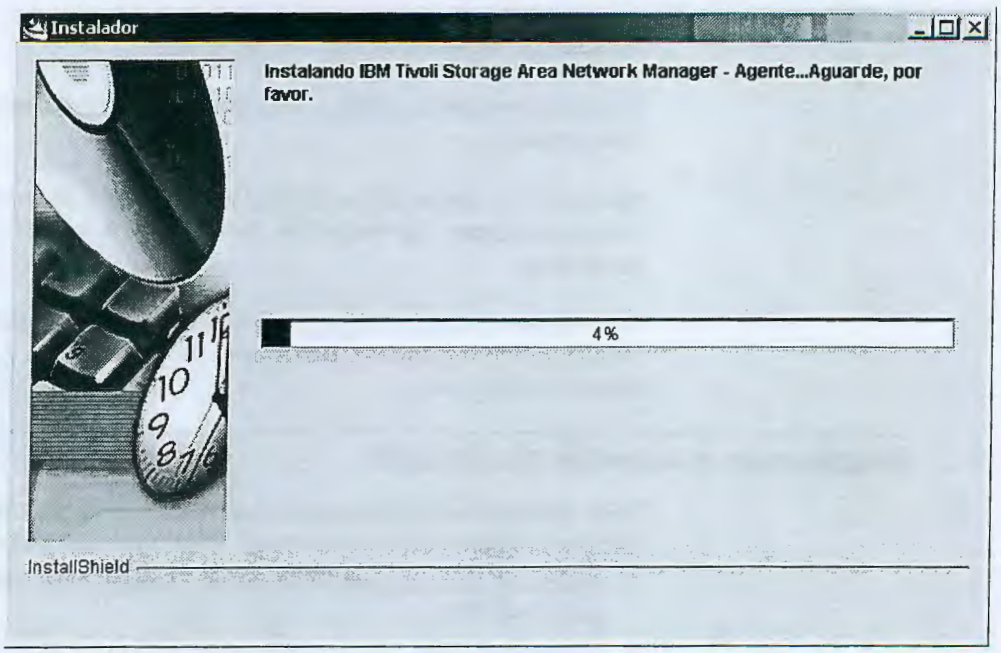


Figura 65. Painel Status

13. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido. Clique em **Concluir** para concluir a instalação.

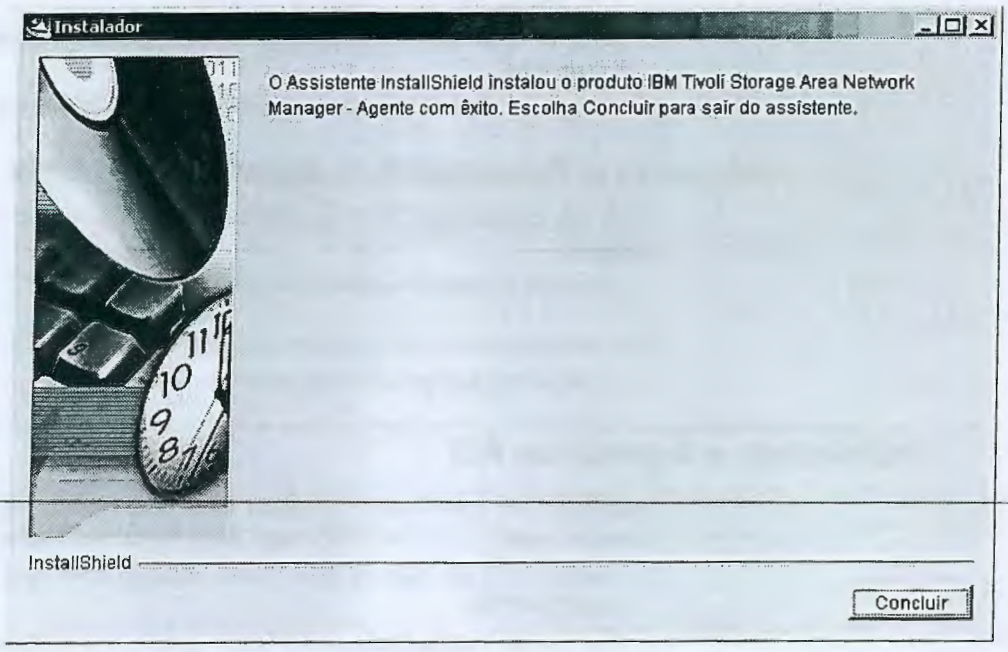


Figura 66. Painel Instalado com Êxito

14. O agente é iniciado automaticamente após a instalação.

ROS nº 03/2005 - CA
CPMI - CORREIOS
Fls. Nº 1549
Doc. 3698

Iniciando e Encerrando o Agente no Windows

Se for necessário iniciar ou encerrar manualmente o agente, clique em:

```
Iniciar → Configurações → Painel de Controle →
Ferramentas Administrativas → Serviços
```

O painel Serviços é exibido. Você pode encerrar ou iniciar o serviço do agente nesse painel.

Para parar o agente, clique com o botão direito do mouse em **Agente ITSANM**. Clique em **Parar**. Um painel de confirmação é exibido indicando que o serviço foi encerrado.

Para iniciar o agente, clique com o botão direito do mouse em **Agente ITSANM**. Dê um clique em **Iniciar**. Um painel de confirmação é exibido indicando que o serviço foi iniciado.

Instalando o Agente no Solaris

Você deve ter autoridade root para instalar o agente. Siga estas instruções para instalar o agente do Tivoli Storage Area Network Manager:

1. Insira o CD do Agente IBM Tivoli Storage Area Network Manager na unidade de CD-ROM.
2. A unidade deve ser montada manualmente. O script de instalação está localizado no diretório do **agente**. Utilize estes comandos para determinar o diretório de montagem (por exemplo, /cdrom/agent) e executar o script de instalação:

```
df -k          (para procurar sistema montado)
cd /cdrom/agent
./setup.sol        (para o Solaris)
```

3. Siga as orientações nos painéis de instalação, começando com a etapa 4 na página 84.
4. O agente é iniciado automaticamente após a instalação.

Iniciando e Encerrando o Agente no Solaris

Caso seja necessário iniciar o agente, acesse o diretório de trabalho e execute este comando:

```
/tivoli/itsanm/agent/bin/solaris2/tcstart.sh
```

Para encerrar os serviços, acesse o diretório de trabalho e execute este comando:

```
/tivoli/itsanm/agent/bin/solaris2/tcstop.sh
```

Instalando o Agente no AIX

Você deve ter autoridade root para instalar o agente. Siga estas instruções para instalar o agente do Tivoli Storage Area Network Manager:

1. Insira o CD do Agente IBM Tivoli Storage Area Network Manager na unidade de CD-ROM.
2. Utilize os comandos a seguir para determinar o diretório de montagem e executar o script de instalação. O script de instalação está localizado no diretório do **agente**. Execute estes comandos:

```
mkdir /cdrom
mount -v'cdrfs' -r'' /dev/cd0 /cdrom
cd /cdrom/agent
./setup.aix
```

3. Siga as orientações nos painéis de instalação, começando com a etapa 4 na página 84.
4. O agente é iniciado automaticamente após a instalação.

Iniciando e Encerrando o Agente no AIX

Para iniciar o agente no AIX, vá para o diretório de trabalho e execute estes comandos (utilizando o diretório padrão):

```
/tivoli/itsanm/agent/bin/aix/tcstart.sh
```

Para encerrar agente no AIX, vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

```
/tivoli/itsanm/agent/bin/aix/tcstop.sh
```

Instalando o Agente no Linux

Antes de instalar o agente do Linux, observe os seguintes requisitos:

- Você deve ter autoridade root para instalar o agente.
- O APMD (Advanced Power Management Daemon) deve estar desativado nas máquinas Linux. O APMD encerra a placa de rede quando o protetor de tela é exibido (após alguns minutos de inatividade). O agente pára a comunicação com o gerenciador quando a placa de rede está desativada.

Siga estas instruções para instalar o agente do Tivoli Storage Area Network Manager:

1. Insira o CD do Agente IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
2. Execute os comandos a seguir. Os comandos criam o diretório de CD-ROM, montam o diretório de CD-ROM, alternam para o diretório do agente, e em seguida executam o script de instalação.

```
mkdir /cdrom
mount /dev/cd0 /cdrom
   cd /cdrom/agent
./setup.lin
```

3. Siga as orientações nos painéis de instalação, começando com a etapa 4 na página 84.
4. O agente é iniciado automaticamente após a instalação.

Iniciando e Encerrando o Agente no Linux

Caso seja necessário iniciar o agente, execute este comando:

```
/tivoli/itsanm/agent/bin/linux/tcstart
```

Para parar o agente, execute este comando:

```
/tivoli/itsanm/agent/bin/linux/tcstop
```

Verificando os Arquivos de Log

Depois de instalar o agente do Windows, verifique este log para determinar se ocorreram erros (utilizando o diretório padrão):

```
c:\tivoli\itsanm\agent\agentLog.txt
```

Depois de instalar o agente do UNIX, verifique este log para determinar se ocorreram erros (utilizando o diretório padrão):

```
tivoli/itsanm/agent/agentLog.txt
```


CPMI - CORREIOS
Fls Nº 1550
Doc. 3698

10203
A.

Capítulo 8. Instalando o Console Remoto do IBM Tivoli Storage Area Network Manager

O console remoto permite acessar o IBM Tivoli Storage Area Network Manager em qualquer local. Se você possui vários operadores que precisam exibir a topologia do ambiente, a existência de vários consoles remotos instalados facilita o acesso para a monitoração desse ambiente.

Você deve ter um ID de usuário do Windows com autoridade administrativa para instalar o console do IBM Tivoli Storage Area Network Manager. Esse console deve ser instalado em uma plataforma Windows 2000 ou XP. Se você tiver o Tivoli NetView 7.1.3 instalado, o IBM Tivoli Storage Area Network Manager configurará o Tivoli NetView, mas não o instalará. Se o Tivoli NetView 7.1.3 não estiver instalado, o IBM Tivoli Storage Area Network Manager instalará o Tivoli NetView.

Nota:

- O IBM Tivoli Storage Area Network Manager *não* oferece suporte para o console da Web Tivoli NetView.
- É necessário parar o Windows Terminal Services antes de instalar o console remoto. Não é possível utilizar o Windows Terminal Services para acessar o console.
- Certifique-se de ter instalado o serviço SNMP e de ter definido o nome da comunidade SNMP como **Público**. Consulte "Etapa 5: Instale o Serviço SNMP" na página 29.
- Se a instalação do console remoto falhar, resolva o problema revendo os arquivos de log. Em seguida reinicialize o sistema para que a instalação parcial com falha seja limpa antes de tentar reinstalar o console remoto. Exclua todos os arquivos abaixo do diretório de instalação base (do console para baixo). Por exemplo, exclua todos os arquivos começando a partir deste diretório para baixo:

  ```
  c:\tivoli\itsanm\console
  ```

Antes de Instalar o Console Remoto

Após instalar o Service Pack 3 para o Windows 2000 nos computadores, é preciso seguir essas etapas para evitar problemas de endereçamento com o Tivoli Storage Area Network Manager. O problema é causado pelo protocolo de resolução de endereços, que retorna o nome abreviado (nome do host incompleto). É possível evitá-lo alterando as entradas nas tabelas de host correspondentes no servidor DNS e no computador local. O nome do host completo deve estar listado antes do nome abreviado. Para corrigir esse problema, siga as etapas em "Alterando o Arquivo HOSTS" na página 206.

© Copyright IBM Corp. 2002, 2003

ROS nº 03/2004 - CN
CPMI - CORREIOS
Fls. Nº 1551
Doc. 3698

Instalando o Console Remoto

Antes de instalar o console remoto, verifique se você possui 150 MB de espaço em disco temporário disponível. É possível localizar o disco temporário informando este comando:

```
echo %TEMP%
```

Siga estas instruções para instalar o console remoto:

1. Se você tiver o Tivoli NetView 7.1.3 instalado, certifique-se de que os seguintes aplicativos estejam encerrados:
   - Web Console
   - Web Console Security
   - MIB Loader
   - MIB Browser
   - Netmon Seed Editor
   - Tivoli Event Console Adaptor Configurator
2. Instale o Serviço SNMP. Consulte "Etapa 5: Instale o Serviço SNMP" na página 29.
3. Insira o CD do Tivoli Storage Area Network Manager Manager and Remote Console na unidade de disco do CD-ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD-ROM do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **launch.exe**.
4. O painel Ativar é exibido. Selecione **Remote Console**. Clique em **Avançar** para continuar.

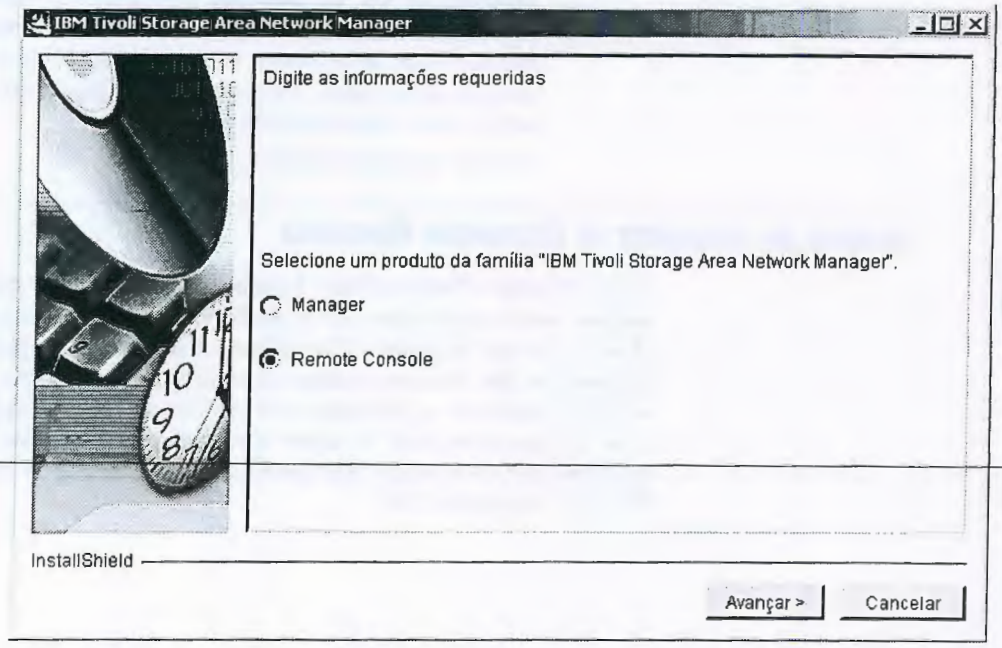


Figura 67. Painel Ativar

5. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para a instalação deste produto.

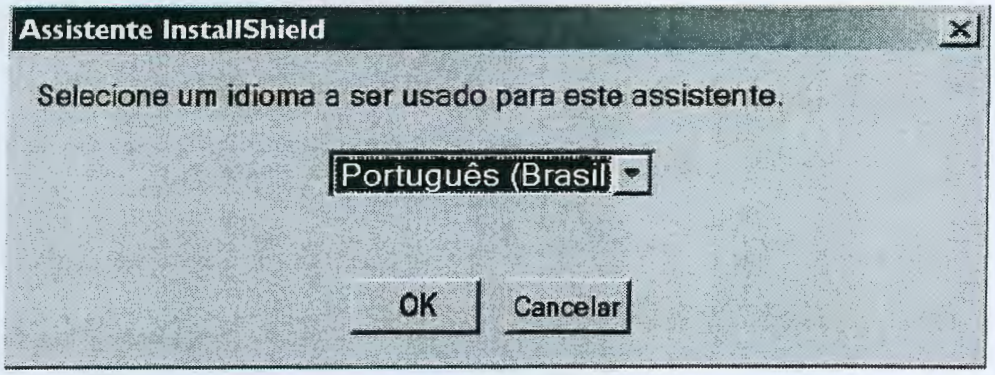


Figura 68. Painel Selecione um Idioma

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

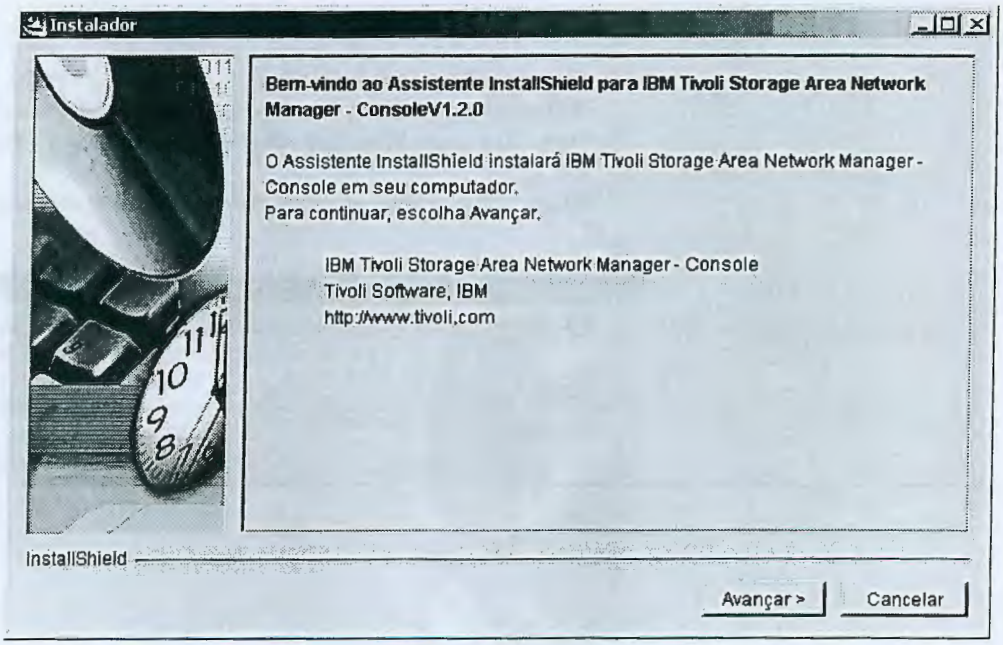


Figura 69. Painel Bem-vindo ao IBM Tivoli Storage Area Network Manager

7. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o IBM Tivoli Storage Area Network Manager.

RQS nº 03/2005 - CPMI
Fls Nº 1552
Doc. 3698

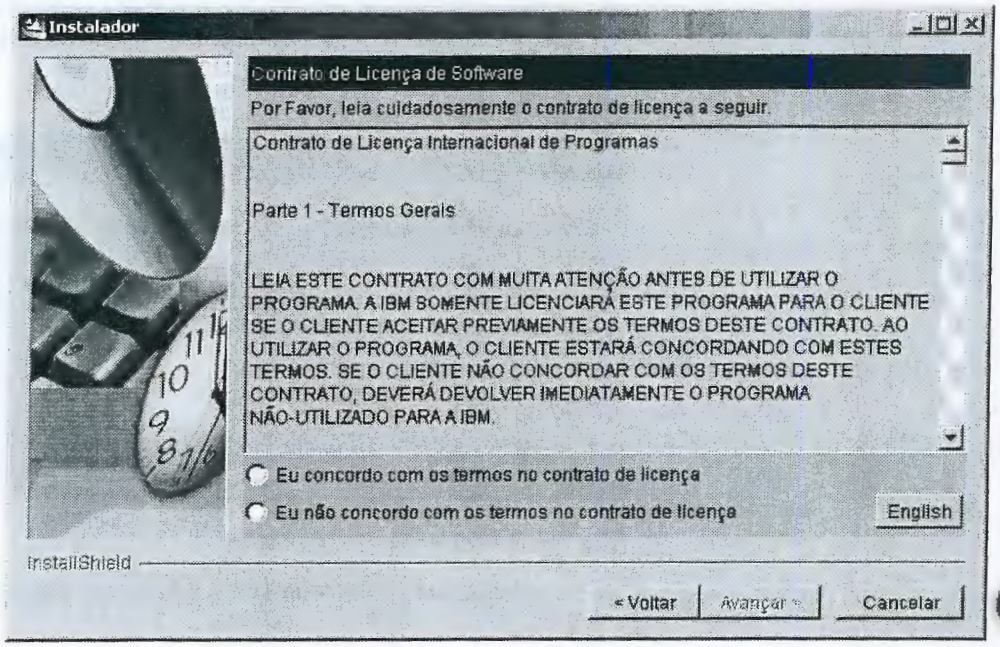


Figura 70. Painel Contrato de Licença de Software

8. O painel Informações sobre o Diretório é exibido. Insira um nome de diretório diferente ou aceite o nome do diretório padrão no qual o IBM Tivoli Storage Area Network Manager será instalado. Clique em **Avançar** para continuar.

   Nota: Não utilize espaços ou hifens em nomes de diretório.

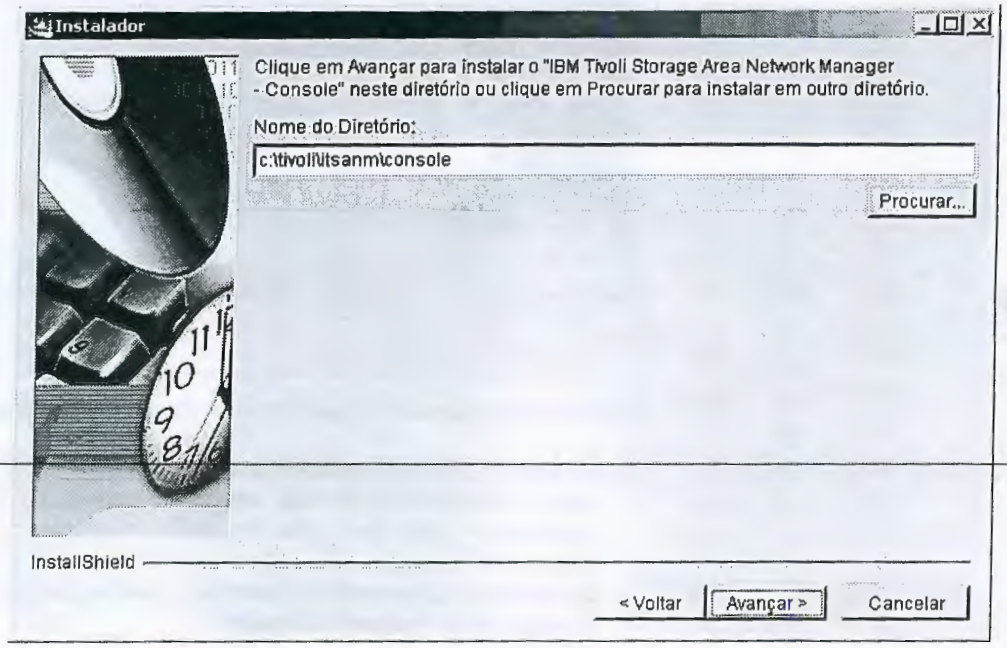


Figura 71. Painel Informações sobre o Diretório

9. O painel Informações sobre o Gerenciador é exibido. Essas informações consistem no nome de host completo e no número de porta base para o computador do gerenciador. O número de porta base é o primeiro número de

porta especificado na etapa 8 na página 67. Insira suas informações e clique em **Avançar** para continuar.

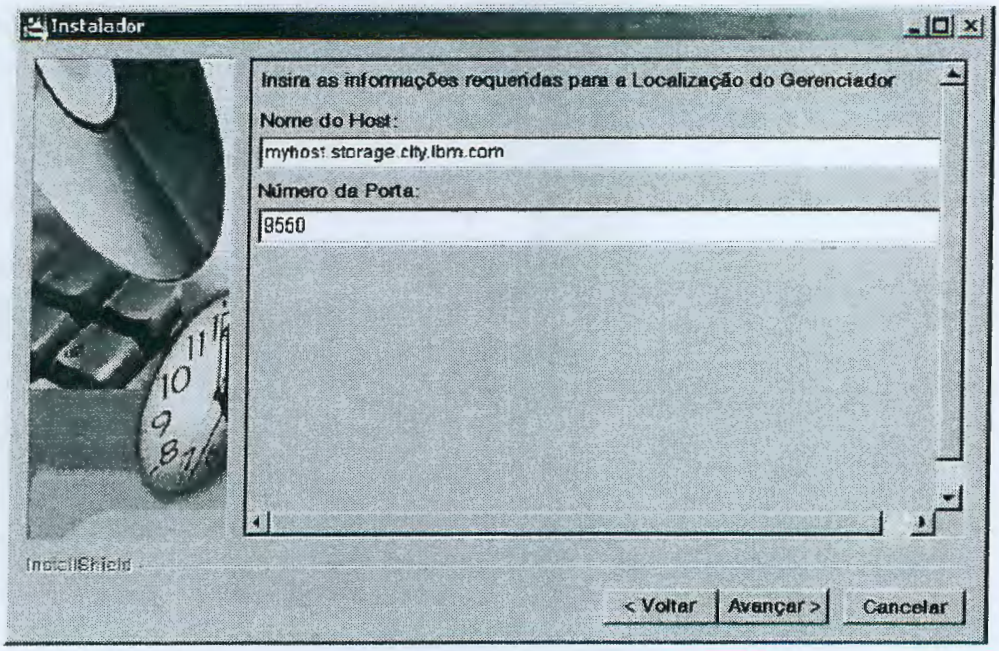


Figura 72. Painel Informações sobre o Gerenciador

10. O painel Número de Porta é exibido. Esse número de porta corresponde a uma faixa de seis números de porta. O número de porta inicial inserido é considerado o *número de porta base*. Para obter informações sobre números de porta, consulte a Tabela 7 na página 20. Insira o número de porta base. Clique em **Avançar** para continuar.

CPMI - CORREIOS
Fls. Nº 1553
Doc 3698

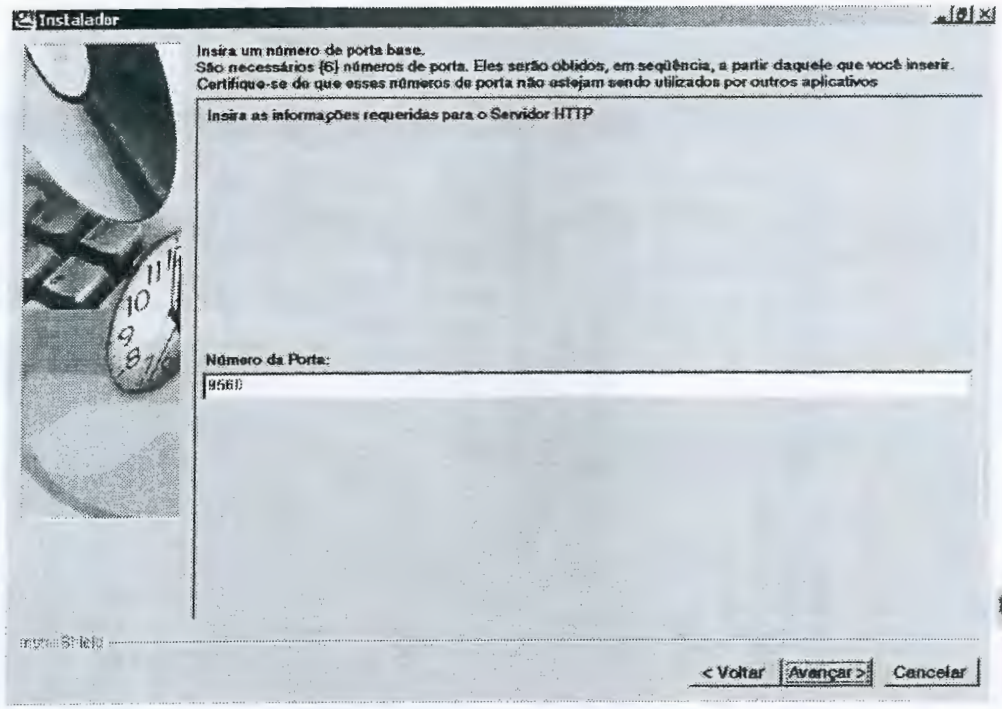


Figura 73. Painel Número de Porta

11. O painel Senha para Autenticação do Host é exibido. Essa senha deve utilizar a mesma senha do gerenciador com o qual este console remoto se comunica. Para obter informações sobre essa senha, consulte a Tabela 12 na página 60. Insira a senha duas vezes. Clique em **Avançar** para continuar.

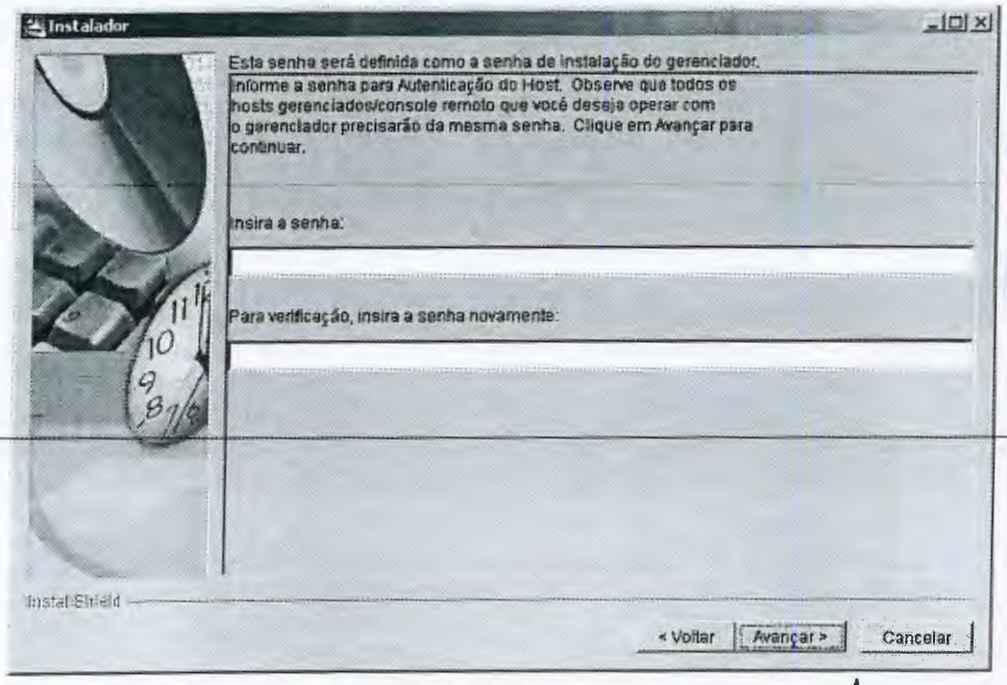


Figura 74. Painel Senha para Autenticação do Host

12. O painel Nome da Unidade do Tivoli NetView é exibido. Insira o nome da unidade na qual você deseja instalar o Tivoli NetView. Clique em **Avançar** para continuar.

    Nota: Esse painel *não* será exibido se o Tivoli NetView 7.1.3 estiver instalado.

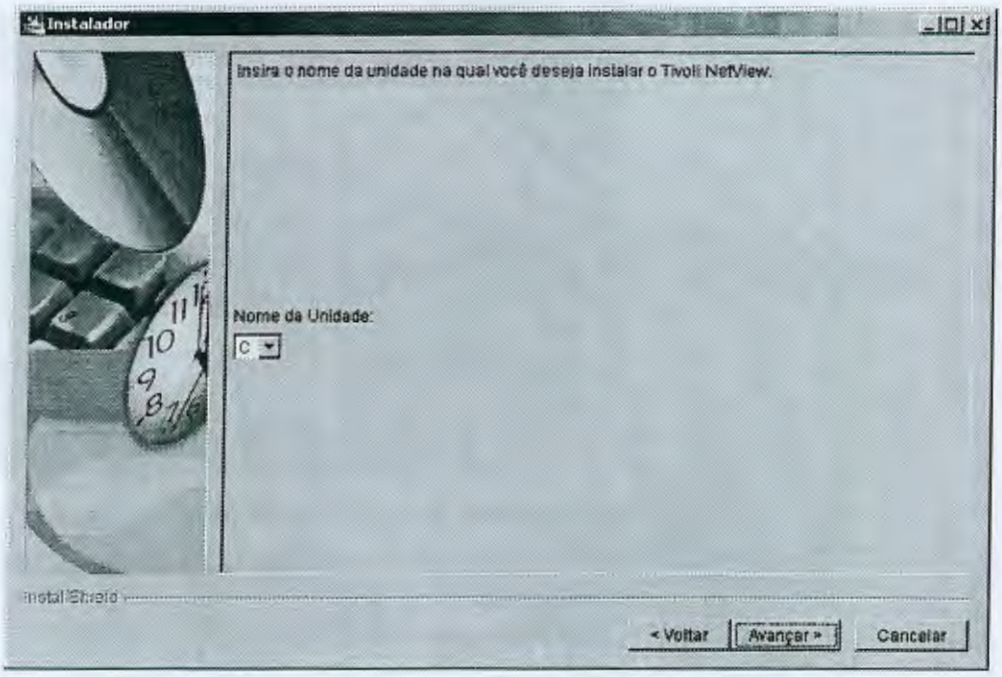


Figura 75. Painel Nome da Unidade do Tivoli NetView

13. O painel Senha do Tivoli NetView é exibido. Para obter informações sobre o ID do usuário e a senha, consulte a Tabela 12 na página 60. Insira a senha duas vezes. Clique em **Avançar** para continuar.

    Nota: Esse painel *não* será exibido se o Tivoli NetView 7.1.3 estiver instalado.

RQS nº 03/2005
Fls Nº 1554
Doc. 3698

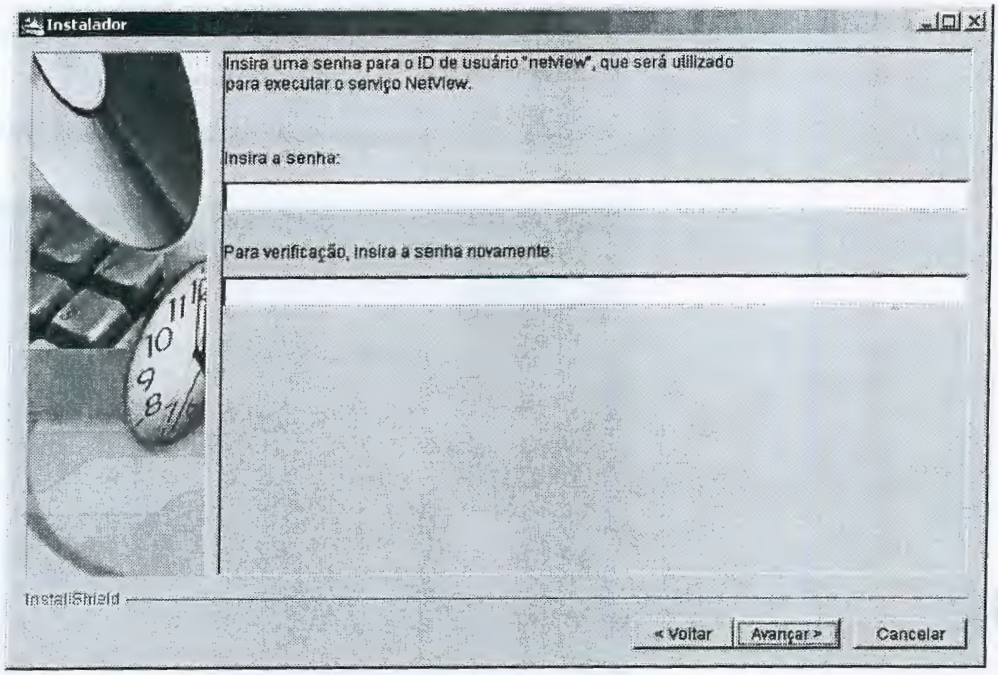


Figura 76. Painel Senha do Tivoli NetView

14. O painel Confirmação da Instalação é exibido. Confirme se o diretório especificado é o local em que você deseja instalar o console. Clique em **Avançar** para continuar.

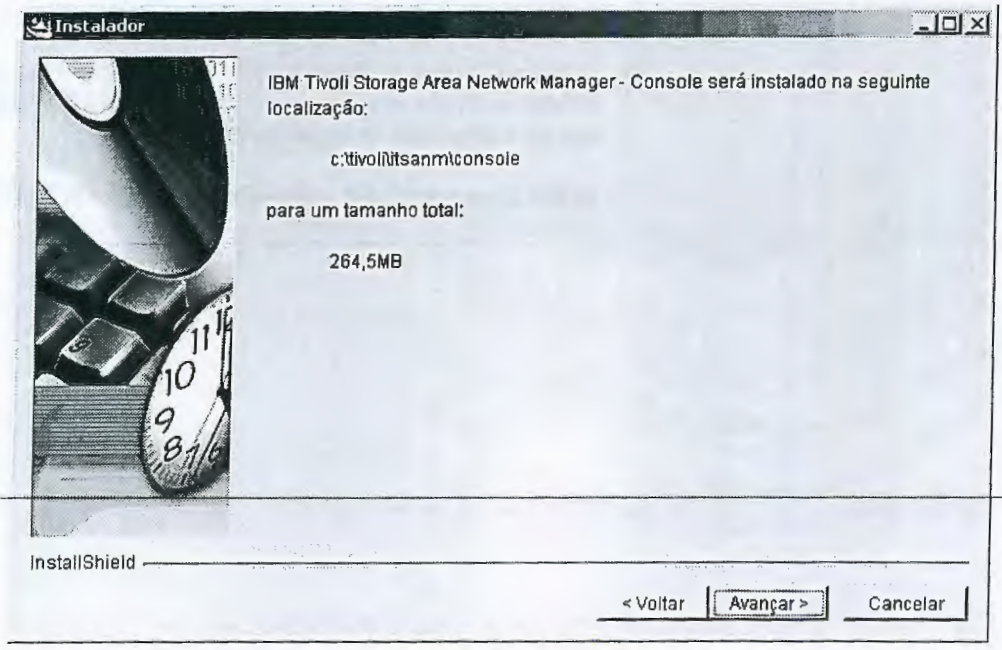


Figura 77. Painel Confirmação da Instalação

15. O painel Status é exibido. Esse procedimento demorará aproximadamente de 15 a 20 minutos. Você verá várias janelas de prompt de comandos se abrindo e fechando durante a instalação.

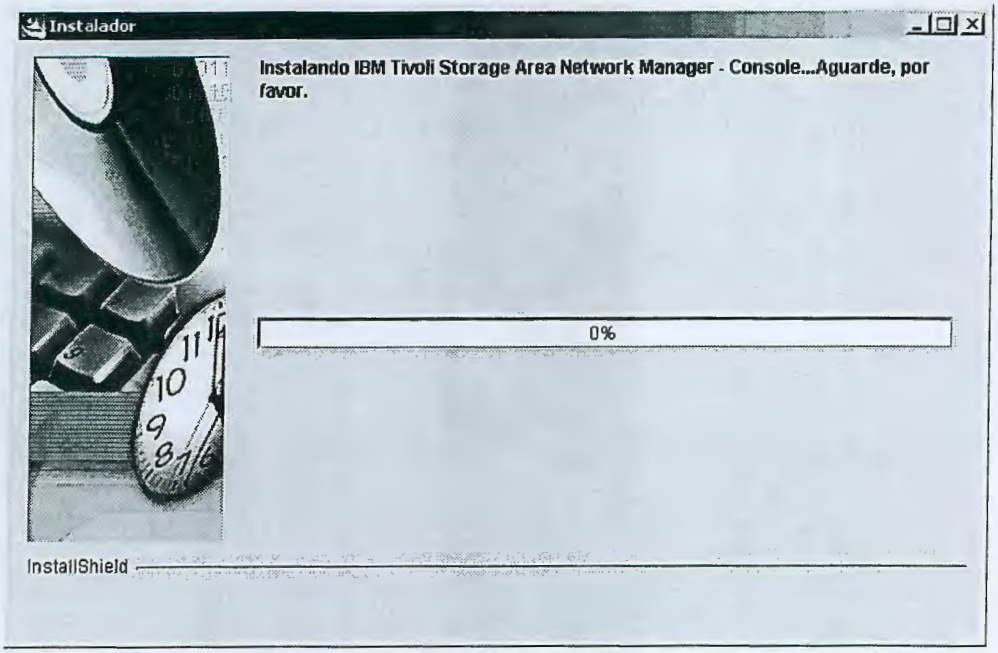


Figura 78. Painel Status

16. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido. Clique em **Avançar** para continuar.

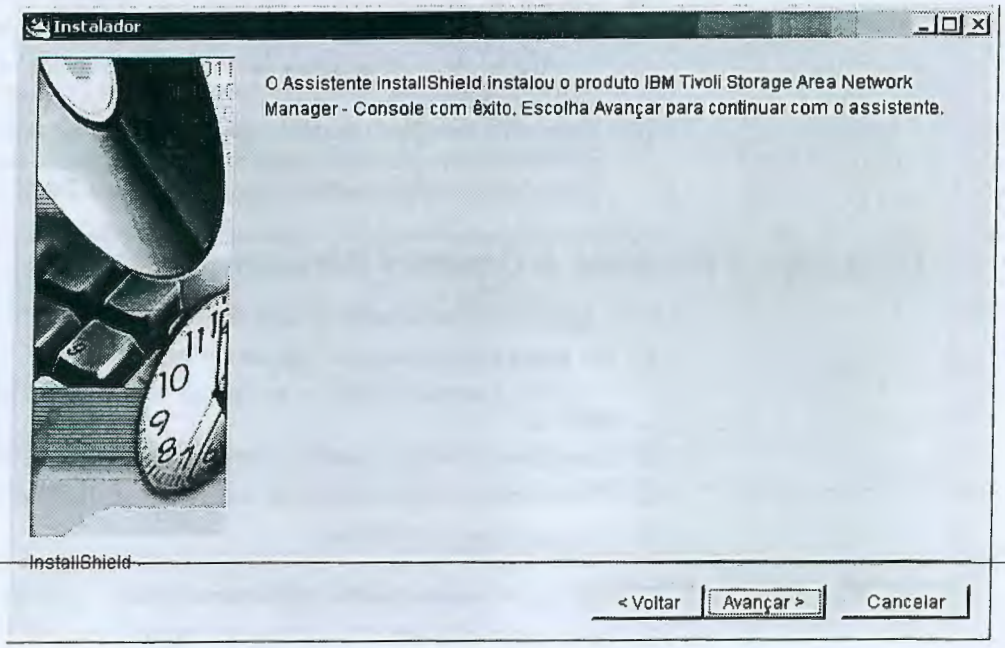


Figura 79. Painel Instalado com Êxito

17. O painel Instalação Concluída é exibido. Para iniciar o computador novamente, clique em **Sim, reinicialize meu sistema.** Clique em **Concluir** para concluir a instalação.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1555
Doc 3698

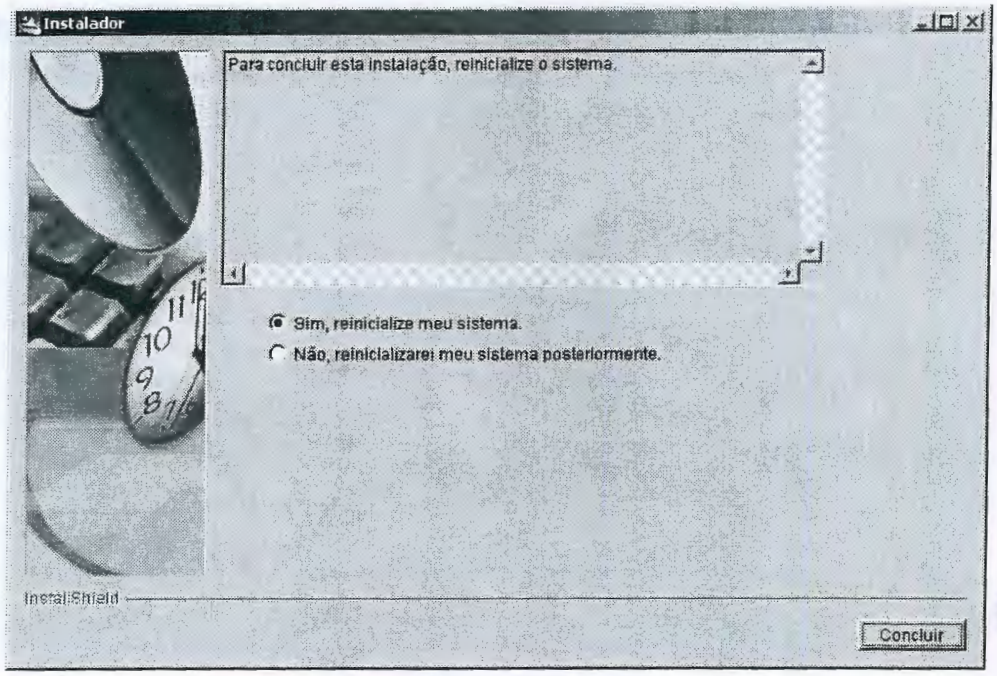


Figura 80. Painel Instalação Concluída

18. Se o painel de prompt na etapa 17 na página 103 não for exibido, você deverá reinicializar o computador. Reinicialize o computador.
19. Depois de reinicializar o computador, verifique se o console do Tivoli Storage Area Network Manager foi iniciado. Clique no seguinte:

    `Iniciar -> Configurações -> Painel de controle -> Ferramentas administrativas -> Serviços (Serviços do NT) -> Console do ITSANM`
20. Depois de instalar o console do IBM Tivoli Storage Area Network Manager, você precisará criar entradas de trap no arquivo trapd.conf do Tivoli NetView. Consulte "Configurando o Arquivo MIB no Tivoli NetView" na página 113.

Iniciando e Parando o Console Remoto

Para iniciar o console remoto, siga estas etapas:

1. Na barra de ferramentas, clique no seguinte:

   `Iniciar -> Definições -> Painel de Controle -> Ferramentas Administrativas -> Serviços`
2. No painel Serviços, localize e destaque **ITSANM – Console**.
3. Clique com o botão direito do mouse em **ITSANM – Console**.
4. Dê um clique em **Iniciar**.

Para parar o console remoto, siga estas etapas:

1. Na barra de ferramentas, clique no seguinte:

   `Iniciar -> Definições -> Painel de Controle -> Ferramentas Administrativas -> Serviços`
2. No painel Serviços, localize e destaque **ITSANM – Console**.
3. Clique com o botão direito do mouse em **ITSANM – Console**.
4. Clique em **Parar**.

Verificando os Arquivos de Log

Depois de instalar o console remoto, verifique este log para determinar se ocorreram erros (utilizando o diretório padrão):

```
c:\tivoli\itsanm\console\log.txt
```

Outros logs recomendados para a verificação de condições de erro são os logs do Tivoli NetView localizados neste diretório padrão:

```
c:\tivoli\itsanm\console\nv\log\*
```

Se você estiver reinicializando o console remoto e o gerenciador estiver sendo executado, você poderá ver essas mensagens de erro:

```
BTASD1863E Ocorreu um erro ao enviar a cadeia por meio de
  socket.com.tivoli.sanmgmt.tsanm.console.network.MsgSendersendCheckMsg
BTASD1865E Ocorreu um erro ao gravar em
  socket.com.tivoli.sanmgmt.tsanm.console.network.ClientSockCleintSock
BTASD1856E A conexão ao daemon do IBM Tivoli NetView é
  down.com.tivoli.sanmgmt.tsanm.console.SanManagerDaemon$MapperWatchThreadrun
```

Estas mensagens são normais neste ambiente.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1556
3698
Doc

Capítulo 9. Configurando o IBM Tivoli Storage Area Network Manager

Esta seção fornece informações sobre as diferentes opções de configuração que podem ser selecionadas, bem como os procedimentos que você pode seguir para atingir esses objetivos.

Siga estas etapas gerais para configurar o IBM Tivoli Storage Area Network Manager:

1. Selecione uma opção de configuração e siga as etapas para concluir a configuração. Consulte "Opções de Configuração" na página 108.
2. Configure os agentes fora de banda. Consulte "Configurando os Agentes Fora de Banda" na página 112.
3. Configure o arquivo mib. Consulte "Configurando o Arquivo MIB no Tivoli NetView" na página 113.
4. Configure o IBM Tivoli Storage Area Network Manager para enviar eventos. Consulte "Configurando o IBM Tivoli Storage Area Network Manager para Enviar Eventos" na página 113.

Outras informações sobre a configuração incluem:

- Configuração de dispositivos para enviar eventos ao Tivoli Enterprise Console. Consulte "Configurando Dispositivos para Enviar Eventos ao Tivoli Enterprise Console" na página 116.
- Configuração do IBM Tivoli Storage Area Network Manager para a descoberta de iSCSI. Consulte "Configurando o IBM Tivoli Storage Area Network Manager para a Descoberta de iSCSI" na página 118.
- Configuração do IBM Tivoli Storage Area Network Manager para EDFI. Consulte "Configurando o IBM Tivoli Storage Area Network Manager para EDFI" na página 123.

Para obter mais informações sobre eventos em banda e traps SNMP fora de banda, consulte "Informações Adicionais" na página 210.

Controlando e Filtrando Eventos

O IBM Tivoli Storage Area Network Manager executa descobertas quando recebe eventos para atualizar as informações no banco de dados. Geralmente, esses eventos são traps SNMP de chaves que indicam as alterações da SAN. Os subsistemas de armazenamento e outros dispositivos podem ser configurados para enviar traps SNMP ao IBM Tivoli Storage Area Network Manager para iniciar novamente o processo discovery de varredura.

Nem todos os traps que podem ser publicados por dispositivos indicam alterações no status da SAN ou na configuração. Por exemplo, muitos dispositivos suportam vários níveis de traps SNMP e a monitoração de parâmetros e contadores internos. Esses traps causariam muitas redescobertas não desejadas pelo IBM Tivoli Storage Area Network Manager. Evite enviar esses traps ao IBM Tivoli Storage Area Network Manager. Isto pode ser configurado no nível do dispositivo ou pode ser filtrado com o Tivoli NetView.

© Copyright IBM Corp. 2002, 2003

CPMI - CORREIOS
Fls. Nº 1557
Doc 3698

O Tivoli NetView fornece um serviço de envio de eventos. Esse ambiente é configurado quando os dispositivos enviam traps SNMP para o Tivoli NetView e o NetView é configurado para enviar traps SNMP ao IBM Tivoli Storage Area Network Manager. Isto permite visualizar os eventos no monitor de eventos do Tivoli NetView. Isto também faz com que o IBM Tivoli Storage Area Network Manager execute uma redescoberta com base na recepção desses eventos.

Os únicos eventos que devem ser encaminhados do Tivoli NetView para o IBM Tivoli Storage Area Network Manager são aqueles que indicam uma alteração no status ou na configuração da SAN. Outros traps proprietários de chaves e dispositivos de armazenamento que indiquem alterações de status ou de configuração da SAN, também devem ser configurados para encaminhamento. Por exemplo, eventos provenientes de um Enterprise Storage Server que indiquem alterações internas, como alterações de configuração de LUN, devem ser encaminhados ao IBM Tivoli Storage Area Network Manager. Isto é importante para a obtenção de informações sobre eventos de nível da LUN.

Opções de Configuração

As seções a seguir fornecem informações sobre as diferentes opções de configuração que podem ser selecionadas. Consulte a Figura 81 durante a leitura dessas opções.

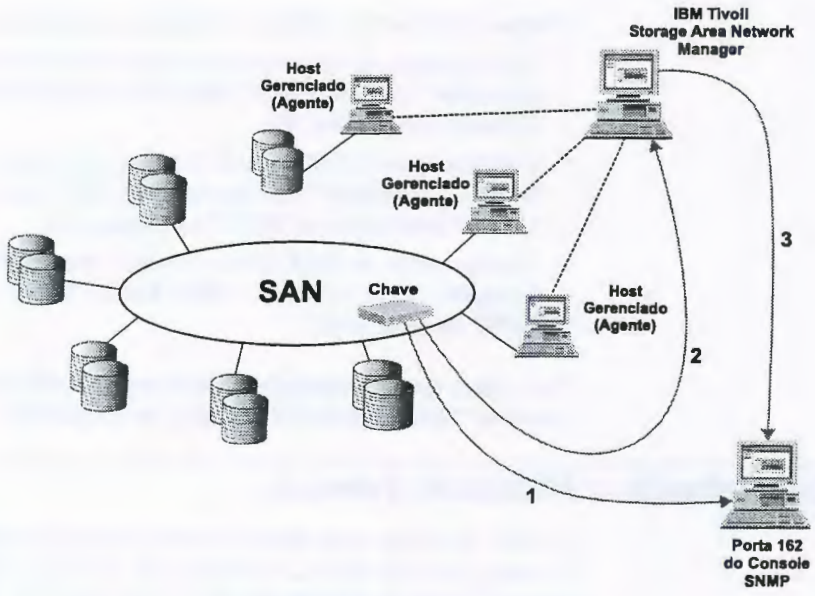


Figura 81. Opções de Configuração do IBM Tivoli Storage Area Network Manager

Configurando Dispositivos e Programas para Enviar Todos os Traps SNMP ao Console Tivoli NetView

Essa é a configuração para a qual o Tivoli Storage Area Network Manager foi desenvolvido para oferecer o melhor suporte. Ela corresponde ao caminho 1 da Figura 81. Nesse caso, o Tivoli NetView é o console SNMP. Por padrão, o Tivoli NetView escuta traps SNMP na porta 162. Vários subsistemas de dispositivos e armazenamento na sua rede de armazenamento podem ser configurados para enviar traps SNMP a esse número de porta. Configure esses dispositivos individuais de forma a apontá-los para a máquina que está executando o Tivoli NetView.

O procedimento abaixo descreve como configurar o IBM Tivoli Storage Area Network Manager para enviar traps ao IBM Tivoli Storage Area Network Manager. Consulte "Configurando Dispositivos para Enviar Traps ao IBM Tivoli Storage Area Network Manager" na página 110. O Tivoli Storage Area Network Manager pode atualizar a exibição da topologia para refletir o status da rede de armazenamento com base nas informações reunidas a parir de seus hosts gerenciados.

Se você também tiver configurado o Tivoli Storage Area Network Manager para enviar traps SNMP ao console Tivoli NetView (caminho 3), essa configuração rastreará todos os traps SNMP na rede de armazenamento. Isso pode ser feito a partir de um único console. O console Tivoli NetView pode ser utilizado como o console de gerenciamento SNMP. Você pode exibir informações sobre dispositivos e monitorar as alterações no status desses dispositivos no Navegador de Eventos do Tivoli NetView.

Se você tiver um gerenciador AIX edesejar gerenciar para receber traps de um processo discovery com base em eventos, então os traps de chave devem ser enviados para a porta 162 em um console do SNMP. Utilize o console remoto em uma máquina Windows como console SNMP. Depois associe este console ao gerenciador AIX. O arquivo `trapfrwd.conf` no console remoto deve ser modificado com o endereço IP do gerenciador AIX (no lugar do host local). A porta é 9556 por padrão.

Procedimento para Configurar Dispositivos e Programas

Se você já tiver o Tivoli NetView instalado e, em seguida, instalar o gerenciador, deverá executar a etapa 1. Para implementar essa configuração, faça o seguinte:

1. Configure o encaminhamento de traps do Tivoli NetView.

   Siga estas etapas para configurar o Tivoli NetView:

   a. Configure o daemon trapfrwd do Tivoli NetView. Edite o arquivo `trapfrwd.conf` no diretório `\usr\ov\conf`. Esse arquivo contém duas seções: a seção Hosts e a seção Traps. Modifique a seção Hosts para especificar o nome do host e a porta para o encaminhamento de traps. Modifique a seção Traps para especificar quais traps devem ser encaminhados pelo Tivoli NetView. Os traps a serem encaminhados para o Tivoli Storage Area Network Manager são:

```
#mgmt
1.3.6.1.2 * (Inclui traps MIB-2 e
             traps FC Management MIB de McDATA)
#experimental
1.3.6.1.3 * (Inclui traps FE MIB e traps FC Management MIB)
1.3.6.1.4 * (Inclui traps MIB de propriedade e traps FC Management MIB de
McDATA)
#Andiamo
1.3.6.1.4.1.9524 *
#Brocade
1.3.6.1.4.1.1588 *
#Cisco
1.3.6.1.4.1.9 *
#Gadzoox
1.3.6.1.4.1.1754 *
#Inrange
1.3.6.1.4.1.5808 *
#McData
1.3.6.1.4.1.289 *
#Nishan
1.3.6.1.4.1.4369 *
#QLogic
1.3.6.1.4.1.1663 *
```


ECT nº 03/2006 - CPMI - CORREIOS
Fls. Nº 1558
Doc 3698

b. Configure o Tivoli NetView para iniciar o daemon trapfrwd. O daemon trapfrwd deve estar em execução antes que os traps sejam encaminhados. O Tivoli NetView não inicia esse daemon como padrão. Para configurar o Tivoli NetView para iniciar o daemon trapfrwd, insira estes comandos:

```
ovaddobj \usr\ov\lrf\trapfrwd.lrf
ovstart trapfrwd
```

Para verificar se o daemon trapfrwd está em execução, clique no seguinte item da barra de menus:

```
Opções → Configuração do Servidor
```

Verifique se o daemon trapfrwd está em execução.

2. Configure o comutador para enviar traps SNMP ao número da porta do console de gerenciamento SNMP. Certifique-se de que o console de gerenciamento SNMP esteja escutando esse número de porta.
3. Configure o console de gerenciamento SNMP para encaminhar traps ao Tivoli Storage Area Network Manager.

Configurando Dispositivos para Enviar Traps ao IBM Tivoli Storage Area Network Manager

É possível configurar os dispositivos na rede de armazenamento para enviar traps SNMP diretamente ao Tivoli Storage Area Network Manager. Essa configuração corresponde ao caminho 2 da Figura 81 na página 108. Configure os dispositivos para enviar seus respectivos traps ao Tivoli Storage Area Network Manager (servidor de gerenciamento). Altere o número da porta no dispositivo. Essa configuração descobre novamente a topologia da rede em resposta aos traps SNMP recebidos. Entretanto, os traps enviados ao Tivoli Storage Area Network Manager não são registrados no Navegador de Eventos do Tivoli NetView. A capacidade de exibir as informações sobre traps em um console não estaria disponível nessa situação. Como alguns dispositivos não oferecem suporte para a alteração do número da porta à qual enviam traps SNMP, essa configuração não está disponível em todos os ambientes de hardware.

Procedimento para Enviar Traps ao Tivoli Storage Area Network Manager

Para implementar essa configuração, siga estas etapas:

1. Configure o comutador para enviar traps à porta do Tivoli Storage Area Network Manager (máquina do gerenciador). O número da porta corresponde ao número de porta base mais 6. Esse número de porta base é especificado durante a instalação da máquina do gerenciador na etapa 8 na página 67. Por exemplo, se você tiver especificado 9550 como o número de porta principal, o comutador deverá ser definido para o número de porta 9550 (9550+6).
2. Defina o nome da comunidade SNMP como PUBLIC, que é o nome padrão. Se você não quiser utilizar esse nome padrão, poderá definir outro nome como o nome da comunidade. Consulte "Alterando o Nome da Comunidade SNMP" na página 208.

Configurando Dispositivos para Enviar Traps ao IBM Tivoli Storage Area Network Manager e ao Console SNMP

Alguns dispositivos podem ser configurados para encaminhar seus traps SNMP a mais de uma localização. Essa configuração corresponde aos caminhos 1 e 2, como mostra a Figura 81 na página 108. Com essa configuração, é possível exibir todos os eventos gerados pelo Tivoli Storage Area Network Manager e pelos dispositivos de

armazenamento. Você pode exibir esses eventos em um console de gerenciamento SNMP comum. O Tivoli Storage Area Network Manager pode responder aos traps SNMP que recebe dos dispositivos na rede de armazenamento. Isso determina o momento em que ele deve descobrir novamente a topologia da rede. Como nem todos os dispositivos oferecem suporte para essa capacidade, essa configuração pode não estar disponível em todos os ambientes.

Procedimento para Enviar Traps ao Tivoli Storage Area Network Manager e ao Console de Gerenciamento SNMP

Para utilizar essa opção, defina o comutador para enviar traps ao console de gerenciamento SNMP e ao IBM Tivoli Storage Area Network Manager.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1559
Doc 3698

Configurando os Agentes Fora de Banda

O IBM Tivoli Storage Area Network Manager utiliza agentes para descobrir o ambiente de armazenamento e monitorar seu status. Utilize o painel Configuração de Agentes para executar os procedimentos a seguir:

- Exibir ou remover agentes em banda inativos
- Exibir, incluir, remover ou configurar agentes fora de banda (agentes SNMP)

É possível acessar o painel Configuração de Agentes (consulte a Figura 82) selecionando o seguinte item no menu do console Tivoli NetView:

```
SAN -► Configurar Agentes
```

Observe que a metade superior do painel mostra os agentes do IBM Tivoli Storage Area Network Manager, enquanto a metade inferior mostra os agentes SNMP.

Figura 82. Painel Configuração do Agente

Os agentes do IBM Tivoli Storage Area Network Manager descobrem informações sobre cada host gerenciado e seu armazenamento local. Os adaptadores de barramento de host no host gerenciado utilizam protocolos de descoberta em banda para reunir informações. Esse painel mostra um agente em cada host gerenciado. Todos os agentes devem estar no estado **Contactado**. É possível remover um agente em banda inativo selecionando esse agente e clicando em **Remover**.

Os agentes SNMP utilizam protocolos de descoberta fora de banda que, por sua vez, utilizam consultas SNMP em uma conexão TCP/IP para reunir informações sobre topologia e atributos. Para incluir um agente SNMP, siga estas etapas:

1. Clique em **Incluir**.
2. A caixa de diálogo Inserir Endereço IP é exibida. Insira um nome ou endereço IP e clique em **OK**.
3. O agente SNMP é incluído na lista de agentes SNMP. O estado desse agente deve ser **Contactado**. Clique em **OK**. Se você não visualizar um estado **Contactado**, verifique se o nome ou endereço IP está correto. Em seguida, verifique se o comutador realmente oferece suporte para descoberta fora de banda.

Nota: O botão **Avançado** é válido somente para comutadores Brocade®. Quando você selecionar um agente no painel Configuração de Agentes e clicar no botão **Avançado**, deverá inserir um ID do usuário e uma senha para o comutador Brocade. Será necessário inserir as informações de login para a conta "admin" no Comutador Brocade. Nenhuma outra conta será suportada.

Depois de inserir o ID do usuário e a senha e o próximo poll ser executado, verifique a seguinte mensagem no log de mensagens:

```
The user ID or password entered for the outband agent target
address <target_address> is incorrect.
```

Se você vir essa mensagem, insira novamente o ID do usuário e a senha corretos.

Configurando o Arquivo MIB no Tivoli NetView

Depois de instalar o Tivoli NetView, você precisará criar entradas de trap no arquivo trapd.conf do Tivoli NetView. *Não* edite o arquivo manualmente. A edição é feita por meio de um arquivo em batch criado pelo programa mib2trap do Tivoli NetView. O arquivo ITSANM.mib está localizado no diretório /misc/utils do CD do Tivoli Storage Area Network Manager. Siga estas etapas:

1. Execute o programa mib2trap no arquivo ITSANM.mib. Especifique o nome completo do caminho para um diretório gravável ao criar o arquivo ITSANM.bat. Por exemplo, execute este comando para criar o arquivo bat no diretório tmp:

   ```
   mib2trap c:\tmp\ITSANM.mib c:\tmp\ITSANM.bat
   ```

   É possível especificar qualquer nome desejado para o arquivo bat. O exemplo a seguir cria o arquivo ITSANM.bat.
2. Execute o arquivo ITSANM.bat.
3. Inicie novamente o Tivoli NetView e torne o monitor visível para ver todos os eventos.

Configurando o IBM Tivoli Storage Area Network Manager para Enviar Eventos

O IBM Tivoli Storage Area Network Manager oferece suporte para a monitoração centralizada de eventos em toda a sua empresa. Se você utiliza um sistema como o Tivoli Enterprise Console ou um aplicativo capaz de receber eventos SNMP, o IBM Tivoli Storage Area Network Manager pode ser facilmente configurado para enviar eventos a esse sistema ou aplicativo. Se você não estiver utilizando um aplicativo

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1560
Doc. 3698

de gerenciamento centralizado no momento, poderá configurar o Tivoli NetView para receber traps SNMP. É possível controlar todos os eventos relacionados à rede de armazenamento detectados pelo IBM Tivoli Storage Area Network Manager no Navegador de Eventos do Tivoli NetView.

A configuração de relatórios de eventos é um processo de duas fases. Em primeiro lugar, é necessário definir o trap SNMP ou o destino do evento do Tivoli Enterprise Console (ou ambos) no painel Destino do Evento para enviar traps e eventos. Em seguida, é necessário configurar o Servidor do Tivoli Enterprise Console ou o aplicativo SNMP (ou ambos) para receber traps e eventos.

Os dispositivos que oferecem suporte para o envio de traps SNMP podem ser configurados para enviar esses traps a um console de traps, como o Tivoli NetView ou o IBM Tivoli Storage Area Network Manager. O envio de traps para o Console Tivoli NetView permite exibir informações sobre traps. Em seguida, é possível tomar decisões com base em informações específicas do fornecedor incluídas no trap. O envio de traps para o IBM Tivoli Storage Area Network Manager possibilita processos de rediscovery automáticos como resultado desses traps.

Durante a instalação, o Console Tivoli NetView é configurado para escutar traps SNMP na porta 162.

Para configurar o IBM Tivoli Storage Area Network Manager para enviar traps SNMP ou eventos do Tivoli Enterprise Console às localizações apropriadas, siga estas etapas:

1. Abra o ícone do Console Tivoli NetView no desktop.
2. No menu Tivoli NetView, clique em:
   `SAN → Definir Destino do Evento`
3. O painel Definir Destino do Evento é exibido.

Figura 83. Painel Definir Destino do Evento

A parte superior do painel permite definir o destino do evento SNMP. Quando você digita um Endereço IP, uma Porta e uma Comunidade, os botões **Incluir** e **Excluir** são ativados. Os campos que podem ser definidos são os seguintes:

Endereço IP
O endereço IP de um host ou um dispositivo que pode receber traps do SNMP.

Porta O número da porta que o host ou o dispositivo utilizará para atender traps do SNMP. O padrão é **162**.

Comunidade
O nome da comunidade à qual o host ou o dispositivo do SNMP é atribuído. O padrão é **Público**.

Utilize o botão **Incluir** para incluir um destino de evento SNMP ao quadro de listagem, na parte superior. Utilize o botão **Excluir** para excluir um destino de evento SNMP da lista.

Se você selecionar **Sim** para ativar o logging do Tivoli Enterprise Console, poderá inserir informações nestes campos:

CPMI - CORREIOS
Fls. Nº 1561
3698
Doc.

IBM Tivoli Enterprise Console
Esse é o endereço IP do seu servidor Tivoli Enterprise Console. Ele será obrigatório se você estiver utilizando o Tivoli Enterprise Console.

Porta do Servidor Tivoli Enterprise Console
Esse é o número da porta do seu servidor Tivoli Enterprise Console. Ele será obrigatório se você estiver utilizando o Tivoli Enterprise Console.

4. Quando terminar de inserir as informações, clique em **OK**.

Configurando Dispositivos para Enviar Eventos ao Tivoli Enterprise Console

O produto Tivoli Enterprise Console é um eficiente aplicativo de gerenciamento de eventos com base em regras que integra o gerenciamento de redes, sistemas, bancos de dados e aplicativos. Ele corresponde ao caminho 3, como mostra a Figura 81 na página 108. Nesse caso, o console SNMP é o Tivoli Enterprise Console. Esse produto oferece uma visão global centralizada da sua empresa de computação ao mesmo tempo em que garante a alta disponibilidade dos recursos de computação e aplicativo. O produto Tivoli Enterprise Console coleta, processa e responde automaticamente a eventos de gerenciamento comuns. Esses eventos de gerenciamento comuns incluem um servidor de banco de dados que não está respondendo, a perda de uma conexão de rede ou um job de processamento em batch concluído com êxito. O Tivoli Enterprise Console age como um ponto de coleta central para alarmes e eventos a partir de várias origens. Essas origens incluem alarmes e eventos de aplicativos Tivoli, aplicativos de associados Tivoli, aplicativos personalizados, plataformas de gerenciamento de redes e sistemas de banco de dados relacional.

O Tivoli Enterprise Console permite processar de forma efetiva o grande volume de eventos em um ambiente cliente/servidor desempenhando as seguintes funções:

- Priorizar eventos de acordo com o nível de importância
- Filtrar eventos redundantes e de baixa prioridade
- Correlacionar eventos a outros eventos de origens diferentes
- Determinar quem deve exibir e manipular eventos específicos
- Iniciar ações corretivas automáticas quando apropriado

Para obter mais informações sobre o Tivoli Enterprise Console, consulte o *Tivoli Enterprise Console: Manual do Usuário*.

Vários dispositivos na rede de armazenamento podem ser configurados para enviar traps SNMP ao número de porta 162. Configure esses dispositivos individuais de forma a apontá-los para a máquina que está executando o Tivoli Enterprise Console. Se você também tiver configurado o Tivoli Storage Area Network Manager para enviar traps SNMP ao Tivoli Enterprise Console, essa configuração rastreará todos os traps SNMP na rede de armazenamento. Isso pode ser feito a partir de um único console.

Configurando o Tivoli Enterprise Console para Receber Eventos do IBM Tivoli Storage Area Network Manager

Para configurar o Tivoli Enterprise Console para receber eventos do IBM Tivoli Storage Area Network Manager, siga estas etapas. O arquivo **ITSANM_120.baroc** está localizado no diretório `/misc/utils` do CD do IBM Tivoli Storage Area Network Manager.

1. No Tivoli Enterprise Console, clique em **Configuração** na barra de menus

2. Clique com o botão direito do mouse em **Operadores**. Inclua você mesmo como o operador. Operadores são usuários que exibem, confirmam e fecham eventos recebidos pelo servidor de eventos.
3. Crie um grupo de eventos denominado ITSANM_Event_Group. Grupos de eventos são utilizados para organizar dados de eventos em exibições diferentes. Também são freqüentemente utilizados para agrupar eventos logicamente de acordo com o tipo, por exemplo, Rede ou Segurança. Grupos de eventos são basicamente um meio de organização e controle do acesso a eventos.

   Para obter mais informações sobre como configurar grupos de eventos e consoles de eventos, consulte a ajuda on-line fornecida com o produto Tivoli Enterprise Console.
4. Crie um console de eventos denominado ITSANM_Console.
5. Atribua ITSANM_Event_Group ao console de eventos.
6. Atribua todas as funções ao Tivoli Enterprise Console: **super**, **sênior**, **admin** e **usuário**. Atribua você mesmo como o operador.
7. Clique no seguinte para visualizar o resumo de eventos:

   `Janelas → Exibição do Quadro de Resumo`

   Dê um clique duplo nessa exibição para tornar visível o Visualizador de Eventos, que contém uma lista de todos os eventos recebidos. É possível clicar em cada evento para exibir seus detalhes.
8. Clique no seguinte para ver a exibição de prioridades:

   `Janelas → Exibição de Prioridades`

   Dê um clique duplo nessa exibição para tornar visível o Visualizador de Eventos, que contém uma lista de todos os eventos recebidos. É possível clicar em cada evento para exibir seus detalhes.

Para ver os eventos do Tivoli Storage Area Network Manager, siga estas etapas:

1. No desktop Tivoli, clique com o botão direito do mouse em:

   `Servidor de Eventos → Bases de Regras`
2. Crie uma nova regra clicando em:

   `Criar → Opção de Base de Regras`

   Nomeie a opção de base de regras. Por exemplo, utilize o nome MeuArmazenamento. Salve essa opção em um diretório da máquina local.
3. Copie a base de regras padrão para a base de regra MeuArmazenamento. Clique com o botão direito do mouse na base de regras padrão e selecione a opção Copiar. Selecione MeuArmazenamento como o base de regras de destino. Selecione as opções Copiar regras e Copiar classes.
4. Importe o arquivo **ITSANM_120.baroc**. Clique com o botão direito do mouse na base de regras MeuArmazenamento e selecione a opção Importar.
5. Na caixa de diálogo Importar Base de Regras de Informações, selecione Importar Definições de Classe.
6. Selecione o arquivo **ITSANM_120.baroc** utilizando o navegador de arquivos.
7. Insira o arquivo de classe importado no final de todos os arquivos baroc listados no quadro de listagem.
8. Compile a base de regras MeuArmazenamento. Clique com o botão direito do mouse na base de regras MeuArmazenamento e selecione à opção Compilar.
9. Carregue a base de regras MeuArmazenamento.
10. Desligue e inicie novamente o Servidor de Eventos.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1564
Doc. 3698

11. Você receberá todos os eventos do Tivoli Storage Area Network Manager no visualizador de eventos.

Eventos do IBM Tivoli Storage Area Network Manager

Os diferentes tipos de classes de eventos que um servidor de eventos pode receber são definidos nos arquivos BAROC (Basic Recorder of Objects in C). Esses arquivos às vezes são referidos como arquivos de definições de classe de eventos. Essas classes são armazenadas em uma base de regra. Quando um o servidor de eventos recebe um evento, a classe do evento é comparada à armazenadas na base de regra ativa. Se a classe de eventos existir na base de regra, o evento será aceito como válido pelo servidor de eventos. Se a classe não existir na base de regra, o evento será descartado.

Uma placa de eventos determina a classe de um evento antes de enviá-lo a um servidor de eventos. Quando um evento nativo é recebido na origem monitorada por uma placa, a placa constrói uma instância do evento da classe de eventos que corresponde ao evento nativo. Isto é baseado em informações sobre a classe de eventos definida em um arquivo BAROC.

As classes de eventos são organizadas em uma hierarquia. Na parte superior da hierarquia está a classe de eventos base, denominada EVENT. As subclasses herdam suas definições de atributos da classe base assim como definem novos atributos.

As classes de eventos e atributos do IBM Tivoli Storage Area Network Manager são mostradas na Tabela 19 na página 214.

Configurando o IBM Tivoli Storage Area Network Manager para a Descoberta de iSCSI

Antes de executar a descoberta de iSCSI, primeiro você deve ativar a descoberta da rede IP. Saiba que quando você ativa a descoberta da rede IP, pode haver muitas atividades, dependendo de quantos dispositivos você pode na rede.

O IBM Tivoli Storage Area Network Manager fornece suporte básico para descoberta e monitoração de dispositivos iSCSI através do Tivoli NetView. O IBM Tivoli Storage Area Network Manager requer o seguinte para a descoberta de iSCSI:

- O dispositivo deve ter o suporte MIB iSCSI e SNMP.
- O dispositivo deve ser configurado de modo que o suporte a iSCSI MIB esteja ativado. Alguns dispositivos não ativam automaticamente o suporte iSCSI (por exemplo, os roteadores do comutador iSCSI). A configuração pode ser feita pela interface de gerenciamento da configuração do dispositivo.
- O dispositivo iSCSI deve ser descoberto primeiro como um dispositivo IP antes que **nvsniffer** possa descobri-lo como um dispositivo iSCSI.

Arquivos MIB iSCSI

Os arquivos MIB iSCSI estão localizados no diretório \usr\ov\snmp_mib. Esses arquivos não são carregados no Tivoli NetView na hora da instalação. Você deve carregar explicitamente esses arquivos MIB utilizando a função de carregamento MIB do NetView. O objetivo de carregar uma MIB é definir os seus objetos para que os aplicativos do programa NetView possam utilizar essas definições da MIB. As MIBs nas quais você tem interesse devem ser carregadas no sistema em que você deseja utilizar o MIB Data Collector ou o MIB Tool Builder. Não é possível

carregar todos os arquivos iSCSI MIB no Tivoli Netview de uma só vez. É necessário excluir o arquivo atual antes de carregar o próximo.

Os arquivos MIB devem ser carregados na seguinte seqüência:
- MIB iSCSI
- MIB Auth iSCSI
- MIB FC_MGMT
- MIB iSNS

Carregue o nível apropriado do arquivo MIB iSCSI que corresponde ao nível do suporte MIB iSCSI no dispositivo iSCSI correspondente que você deseja procurar.

Para carregar ou descarregar MIBs, siga estas etapas:

1. Abra o ícone do Console Tivoli NetView no desktop.
2. No menu Tivoli NetView, selecione:
   `Ferramentas -> MIB -> Loader SNMP V1`
3. O painel do MIB Loader é exibido. Para carregar uma MIB, clique no botão **Carregar**. Para descarregar, selecione uma MIB e clique em **Descarregar**.
4. Se estiver carregando uma MIB, o painel Carregar será exibido. Realce a MIB que deseja e clique em **Abrir**. A MIB será carregada no Tivoli NetView. Você verá o indicador de carregamento da MIB para carregá-la. Esse processo deve ser repetido para carregar as MIBs na ordem de suas interdependências.

Ativando a Descoberta da Rede IP

Para ativar a descoberta da rede IP, siga estas etapas:

1. Abra o Console do Tivoli NetView no desktop.
2. No menu Tivoli NetView, selecione:
   `Opções -> Polling`

RQS nº 03/2003
CPMI - CORREIOS
Fls. Nº 1563
Doc. 3698

Figura 84. Menu do Tivoli NetView

3. O painel Opções de Polling é exibido. Selecione **Poll All Nodes**. Clique em **OK**.

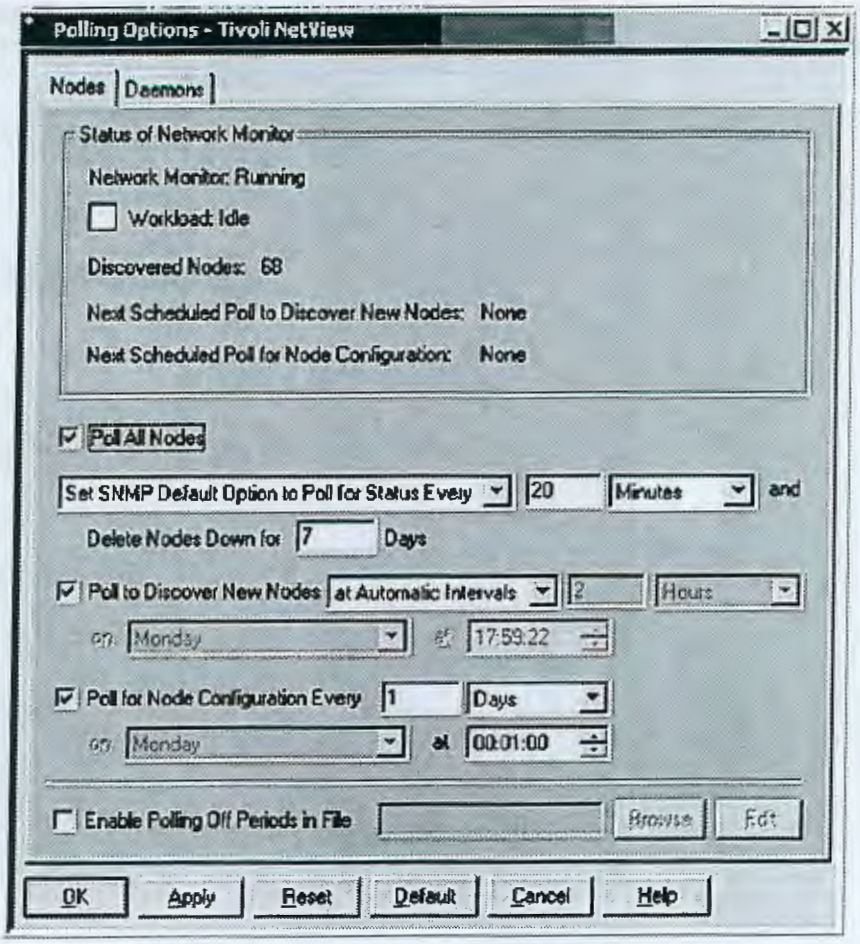


Figura 85. Painel Polling Options

Iniciando a Descoberta iSCSI

Para iniciar a descoberta do iSCSI, siga as próximas etapas. Observe que se você já estiver executando uma descoberta iSCSI, iniciá-la novamente ativará outra instância do programa **nvsniffer**. O tempo de polling padrão é a cada 60 minutos. Para alterar o tempo de polling, consulte o comando **nvsniffer** no *IBM Tivoli Storage Area Network Manager: Guia do Usuário.*

Para iniciar a descoberta iSCSI, siga estas etapas:

1. Vá para o menu Tivoli NetView e selecione:

```
Ferramentas -> Operações iSCSI -> Descobrir Todos os Dispositivos iSCSI
```

Somente é preciso iniciar a descoberta iSCSI uma vez. Se você selecionar esta opção uma segunda vez, terá várias descobertas em andamento. Esta ação pode produzir resultados inesperados.

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 1704
Doc. 3698

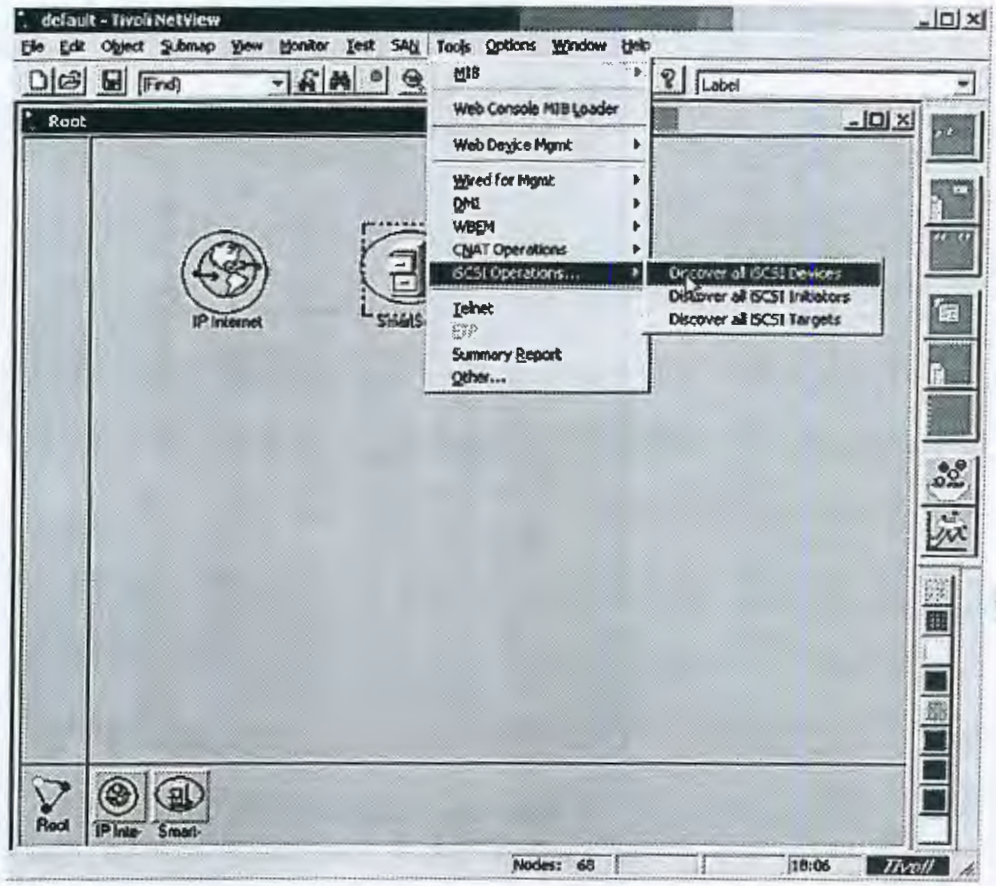


Figura 86. Iniciando a descoberta iSCSI

O tempo de polling padrão é a cada 60 minutos. Se você desejar alterar o tempo de polling, utilize o comando **nvsniffer**. Para obter informações sobre o comando **nvsniffer**, consulte *IBM Tivoli Storage Area Network Manager: Guia do Usuário*.

2. O processo de descoberta cria um SmartSet. Para obter um exemplo de um SmartSet, consulte Figura 87. Dê um clique duplo no iSCSI para visualizar seus membros.

Figura 87. Exemplo de SmartSet iSCSI

3. Dê um clique duplo no SmartSet iSCSI para visualizar o dispositivo iSCSI.

Parando a Descoberta iSCSI

Para parar a descoberta iSCSI, utilize o comando **at** do Windows. A seguir, um exemplo do comando **at**:

```
at <ID_do_job> /d
```

Em que *ID_do_job* indica o ID do job de descoberta iSCSI (programa **nvsniffer**) que você desejar parar. Você deve parar todas as instâncias dos programas **nvsniffer** que estão sendo executados. Você pode executar um comando **at** separado para cada programa que deseja parar.

Você pode obter o *ID_do_job* clicando na barra de tarefas e depois em **Gerenciador de Tarefas**. Clique na guia Processos. Localize **nvsniffer.exe**. A coluna PID identifica o *ID_do_job* de **nvsniffer.exe** para uso no comando **at**. Você também pode parar **nvsniffer.exe** no painel do Gerenciador de Tarefas realçando-o e dando um clique com o botão direito do mouse nele e depois em **Concluir Processo**.

Para obter informações sobre como planejar novamente a descoberta iSCSI, consulte o comando **nvsniffer** no *IBM Tivoli Storage Area Network Manager: Guia do Usuário*.

Configurando o IBM Tivoli Storage Area Network Manager para EDFI

A função EDFI executa a análise de falhas previstas nos links de interconexão da SAN do Fibre Channel, à procura de problemas potenciais. Para utilizar a função EDFI é necessário que ela seja configurada adequadamente. Primeiro, carregue um conjunto de regras e depois inicie a EDFI. Você pode selecionar o conjunto de regras adequado para a sua empresa.

É altamente recomendável que a EDFI seja desativada durante a instalação e a reconfiguração de hardware da SAN. Isto evitará que apareçam eventos falsos de erros nos logs de propriedades da EDFI assim como nos ícones do NetView.

Carregando um Conjunto de Regras

Um aspecto chave da configuração da EDFI é o conjunto de regras. Os conjuntos de regras contêm os limites e critérios específicos utilizados pela análise de falhas previstas e funções associadas de isolamento de falhas do IBM Tivoli Storage Area Network Manager. Os produtos de hardware são alterados com freqüência e os conjuntos de regras permitem que o IBM Tivoli Storage Area Network Manager acompanhe todas as alterações específicas necessárias para a EDFI. Recomenda-se que os conjuntos de regras disponíveis com o IBM Tivoli Storage Area Network Manager sejam verificados com relação aos conjuntos de regras recomendados disponíveis no site de suporte do IBM Tivoli Storage Area Network Manager. Se o site recomendar um conjunto de regras diferente, copie-o para o diretório apropriado na máquina do gerenciador. Depois que o conjunto de regras estiver no diretório adequado, ele aparecerá automaticamente na lista de conjuntos de regras disponíveis para seleção.

Se uma nova regra for copiada para o diretório correto mas não aparecer na lista de regras disponíveis para seleção, ela pode ter sido danificada. Os testes de consistência da EDFI verifica a existência de regras danificadas. As regras danificadas resultarão em uma entrada no arquivo `msgITSANM.log`.

No Windows, o conjunto de regras está localizado no diretório <install_dir>\conf\edfi. Por exemplo:

```
C:\tivoli\itsanm\manager\conf\edfi
```

No AIX, um exemplo de diretório do conjunto de regras é o seguinte:

```
/tivoli/itsanm/manager/conf/edfi
```

Os conjuntos de regras são identificados pelos seguintes campos:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1595
Doc. 3698

Estado

O estado é definido como:

Ativo O conjunto de regras com o estado ativo está sendo utilizado atualmente pela EDFI. Somente um conjunto de regras pode estar ativo por vez.

Não Ativo

O conjunto de regras não está selecionado e atualmente não está sendo utilizado pela EDFI.

Selecionado

O conjunto de regras foi selecionado. Somente um conjunto de regras pode ser selecionado por vez. No estado selecionado, o conjunto de regras está qualificado para se tornar o conjunto de regras ativo, isso é possível clicando-se no botão **Aplicar** ou **OK**.

Arquivo

Nome do arquivo no sistema de arquivos local.

Versão

O número da versão do conjunto de regras. O número da versão está no formato de XX.YY.ZZ, em que:

- XX – é o número da revisão principal.
- YY – é o número da revisão secundário.
- ZZ – é o número da revisão incremental.

Descrição do Conjunto de Regras

Um nome resumido que identifica o conjunto de regras. Ele descreve resumidamente as características exclusivas do conjunto de regras.

Iniciando e Parando a EDFI

Para iniciar a EDFI, siga estas etapas:

1. Abra o ícone do Console Tivoli NetView no desktop. No menu Tivoli NetView, selecione:

   `SAN -► Configuração ED/FI`

10172

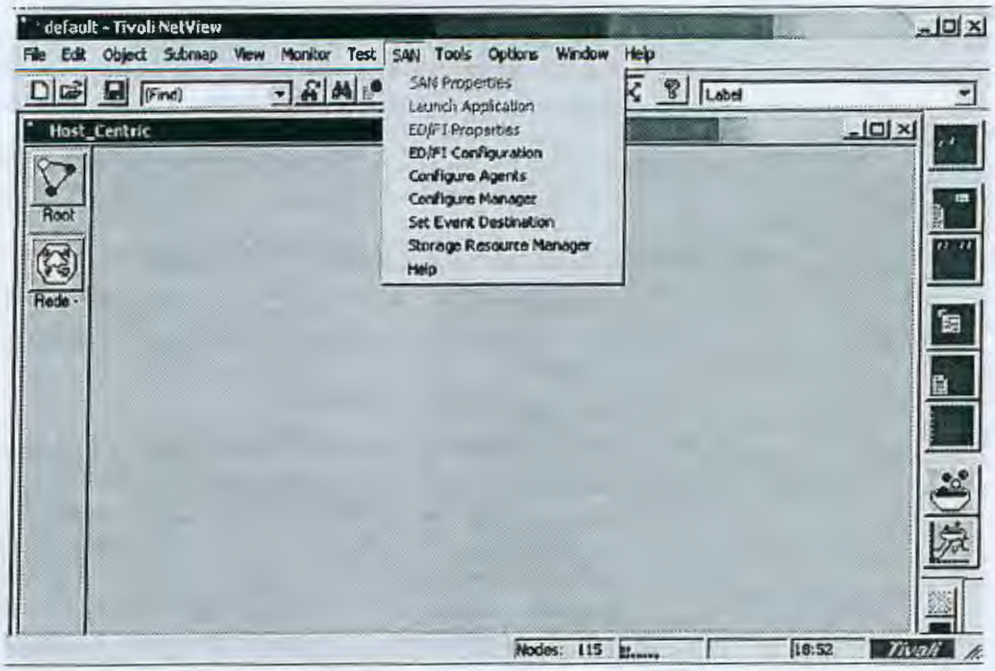


Figura 88. Menu do Tivoli NetView

2. É exibido o painel de Configuração EDFI. Certifique-se de que o botão de opções Ativar Detecção de Erro e Isolamento de Falha esteja selecionado. Clique em **OK** ou **Aplicar**.

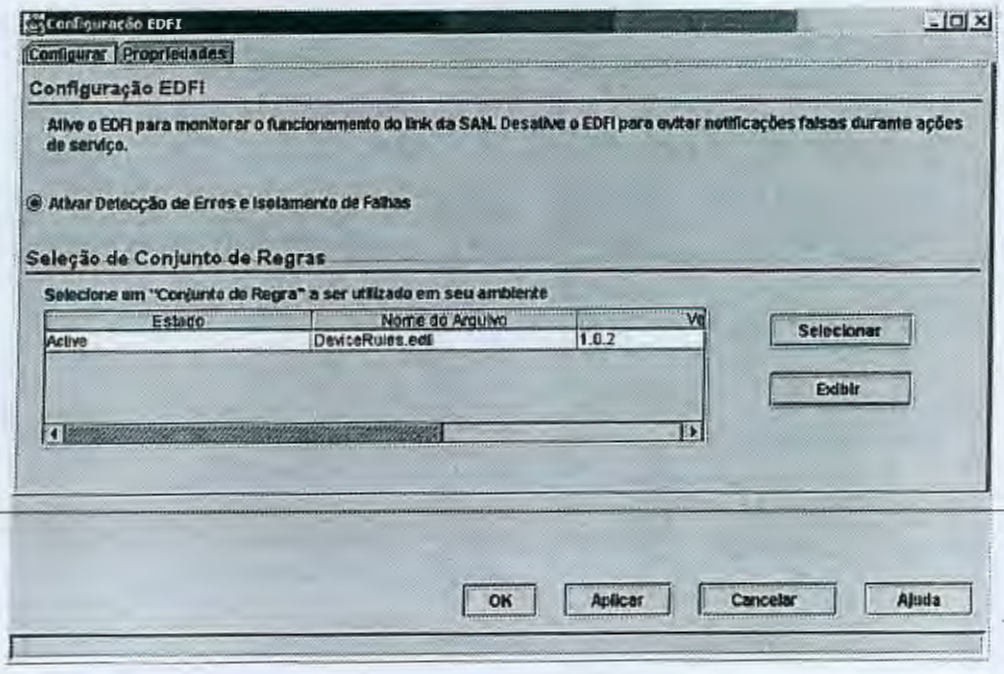


Figura 89. Painel de Configuração de EDFI

Para parar a EDFI, faça o seguinte:

1. Abra o ícone do Console Tivoli NetView no desktop. No menu Tivoli NetView, selecione:

RQS nº 03/2005
CPMI CORREIOS
Doc. 3698

SAN -> Configuração ED/FI

2. No painel Propriedades de Configuração de EDFI, desmarque o botão de opções Ativar Detecção de Erros e Isolamento de Falha. Clique em **OK** ou **Aplicar** para consolidar a alteração.

Nota: Para evitar que notificações de erro falsas apareçam na SAN, desative a EDFI durante a instalação e reconfiguração de hardware da SAN.

Selecionando um Conjunto de Regras

Para selecionar um conjunto de regras, siga estas etapas:

1. Abra o ícone do Console Tivoli NetView no desktop. No menu Tivoli NetView, selecione:

   SAN -> Configuração ED/FI

2. O painel Propriedades de Configuração de EDFI é exibido.
3. Depois que o conjunto de regras estiver no diretório adequado, ele aparecerá automaticamente na lista de conjuntos de regras disponíveis para seleção. Consulte Figura 89 na página 125. No painel Propriedades de Configuração da EDFI, realce o conjunto de regras desejado e clique no botão **Selecionar**. Em seguida, clique em **OK** ou **Aplicar** para consolidar a alteração.
4. Você poderá exibir um conjunto de regras realçando um no painel Propriedades de Configuração da EDFI e clicando no botão **Exibir**. O painel Regras da EDFI é exibido. Um exemplo de um painel de regras é mostrado na Figura 90.

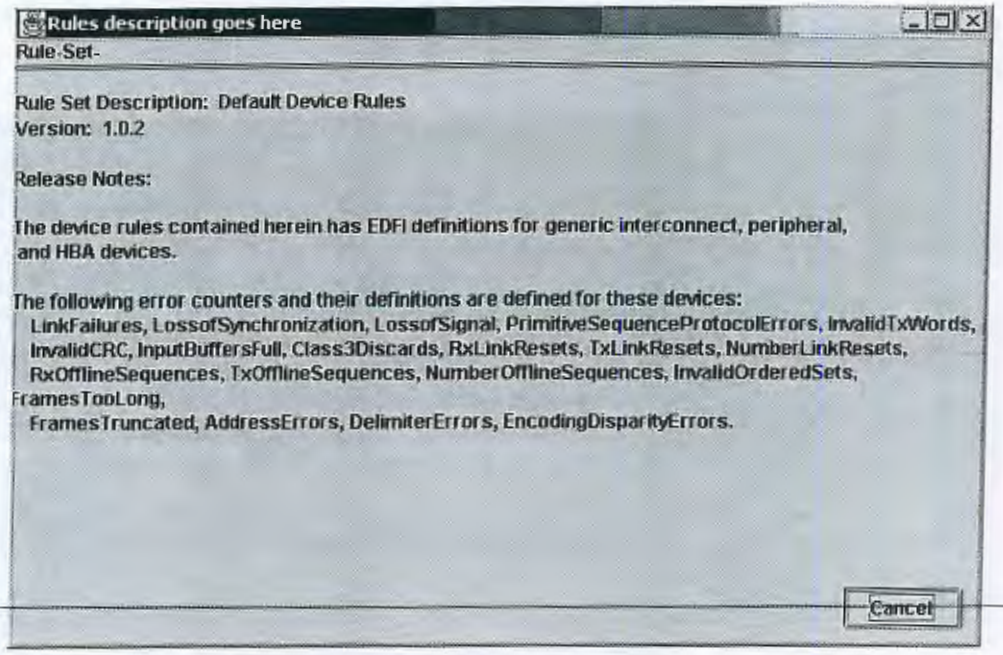


Figura 90. Exemplo do Painel Regras da EDFI

Relatório de Eventos EDFI

A EDFI gera eventos padrões do Tivoli Enterprise Console que podem ser utilizados para fins de relatório. Os tipos de eventos para a EDFI são:

Início do Serviço EDFI
Esse evento é emitido quando a EDFI tiver sido iniciada com êxito.

Parada do Serviço EDFI
Este evento é emitido quando a EDFI foi parada.

Notificação do Dispositivo EDFI
Este evento é emitido quando a EDFI tiver uma notificação para relatar.

Limpeza da Notificação do Dispositivo EDFI
Esse evento é emitido quando o evento tiver sido limpo.

Os OIDs (Identificadores de Objetos) desses eventos são os seguintes:

Tabela 14. OIDs (Identificadores de Objetos)

Evento	OID
Início do serviço EDFI	1.3.6.1.4.1.2.6.173.5.1
Parada do serviço EDFI	1.3.6.1.4.1.2.6.173.5.2
Notificação do dispositivo EDFI	1.3.6.1.4.1.2.6.173.3.36
Limpeza da notificação do dispositivo EDFI	1.3.6.1.4.1.2.6.173.3.36

Para obter mais informações sobre o relatório de erro e a configuração do relatório de eventos da EDFI, consulte *IBM Tivoli Storage Area Network Manager: Guia do Usuário.*

Configurando uma SAN sem Hosts Gerenciados

Há casos em que podem não existir agentes na SAN. Estes casos são:

- Os hosts não têm atualmente um agente instalado.
- O sistema operacional do host não é suportado pelo agente IBM Tivoli Storage Area Network Manager.
- Os requisitos do cliente não exigem a implementação de um agente IBM Tivoli Storage Area Network Manager (somente o mapa de topologia).

Nestes casos, recomenda-se que um agente seja instalado no próprio IBM Tivoli Storage Area Network Manager (componente do gerenciador). Isto permite que o IBM Tivoli Storage Area Network Manager utilize os recursos avançados como RNID (Remote Node Identification) e a coleta de dados da EDFI do dispositivo que requer um agente. Consulte Figura 91.

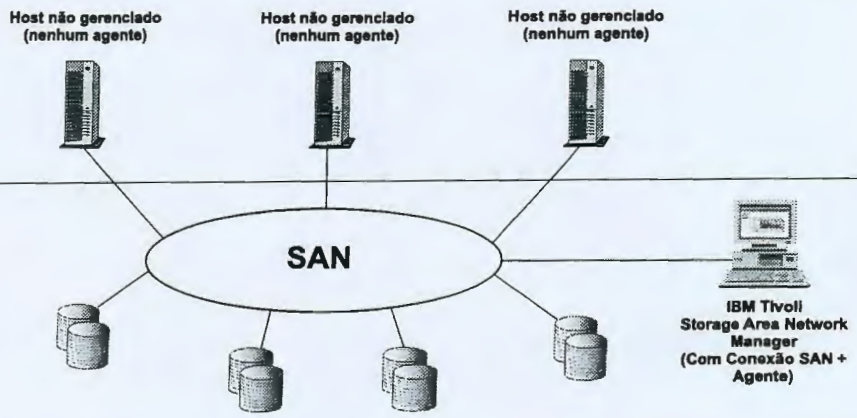


Figura 91. IBM Tivoli Storage Area Network Manager – Gerenciando uma SAN sem Hosts Gerenciados

RQS nº 03/2005
CPMI - CORREIOS
Fls. Nº 3698
Doc. 3698

Normalmente o gerenciador não tem uma placa do barramento do host Fibre Channel. Nesta configuração, são seguidas as etapas:

1. Uma placa do barramento do host Fibre Channel é adicionada ao gerenciador.
2. Um agente é instalado no gerenciador. (O gerenciador é instalado primeiro).
3. Todos os dispositivos de armazenamento são verificados para assegurar que utilizem as técnicas de mascaragem de LUN. Essas técnicas evitam que o IBM Tivoli Storage Area Network Manager acesse os discos utilizados pelos sistemas host.
4. A placa do barramento do host Fibre Channel é anexada à SAN que será gerenciada. Esse host é adicionado a cada zona que deve ser gerenciada pelo IBM Tivoli Storage Area Network Manager.

Capítulo 10. Fazendo Upgrade do IBM Tivoli Storage Area Network Manager

Esta seção descreve como fazer upgrade do IBM Tivoli Storage Area Network Manager da versão 1.1.0 ou 1.1.1 para a versão 1.2.0.

Para utilizar o mesmo banco de dados da versão 1.1.0 ou 1.1.1, você deve especificar o mesmo nome do banco de dados e o ID do usuário e a senha do DB2 que especificou quando instalou a versão anterior.

Estas são as alterações que ocorrerão na instalação do IBM Tivoli Storage Area Network Manager:

- Será feito o upgrade do JVM 1.3.0 para 1.3.1.
- Será feito o upgrade do Tivoli NetView de 7.1.1 para 7.1.3 para o gerenciador e o console remoto do Windows.
- O MQSeries será removido.
- O WebSphere Application Server será substituído pelo Embedded WebSphere Application Server – Express, Versão 5.0 no gerenciador.

Fazendo o Upgrade do Gerenciador do Windows

Para fazer o upgrade do gerenciador do Windows, siga estas etapas:

1. É necessário ter um ID de administrador do DB2 para fazer o upgrade do Tivoli Storage Area Network Manager.
2. Se o DB2 FixPak 8 não tiver sido instalado, instale-o agora. Consulte "Fazendo o Upgrade do DB2 com o FixPak 8" na página 28.
3. Se o Tivoli NetView 7.1.3 estiver instalado, certifique-se de que os seguintes aplicativos estejam encerrados:
   - Web Console
   - Web Console Security
   - MIB Loader
   - MIB Browser
   - Netmon Seed Editor
   - Tivoli Event Console Adaptor Configurator

   Além disso, certifique-se de que os Serviços de Terminal do Windows 2000 não estejam em execução.
4. Insira o CD do Tivoli Storage Area Network Manager (Manager and Remote Console) na unidade de disco de CD-ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD-ROM do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **launch.exe**. O painel Ativar é exibido. Selecione **Manager**. Clique em **Avançar** para continuar.

© Copyright IBM Corp. 2002, 2003

ECT/ECO nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1568
Doc. 3698

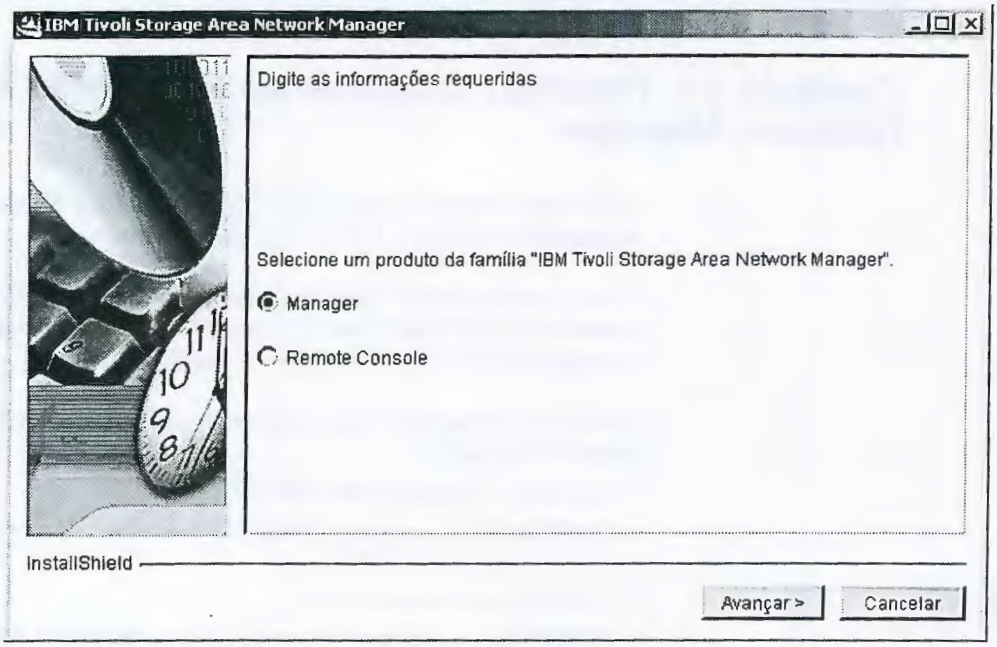


Figura 92. Painel Ativar

5. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para fazer o upgrade desse produto.

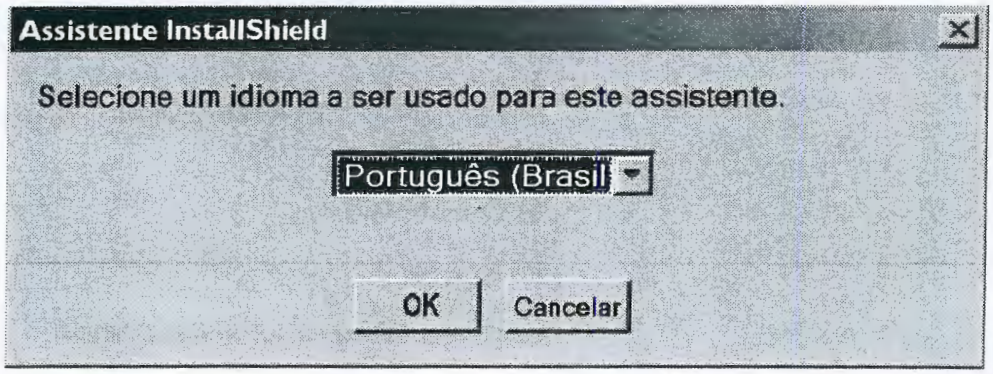


Figura 93. Painel Selecione um Idioma

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

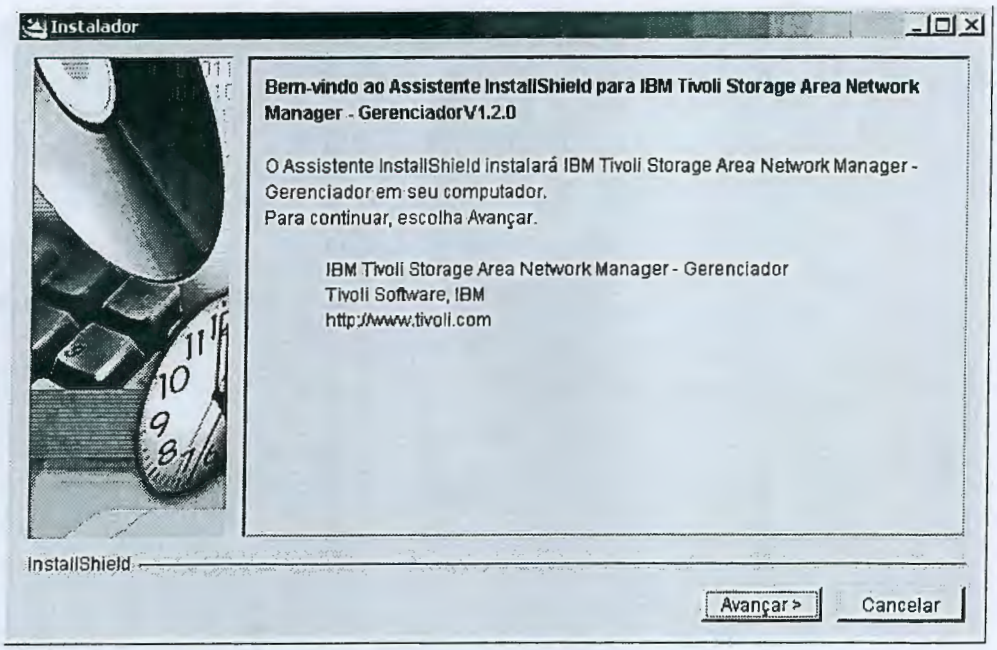


Figura 94. Painel Bem-vindo ao IBM Tivoli Storage Area Network Manager

7. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o Tivoli Storage Area Network Manager.

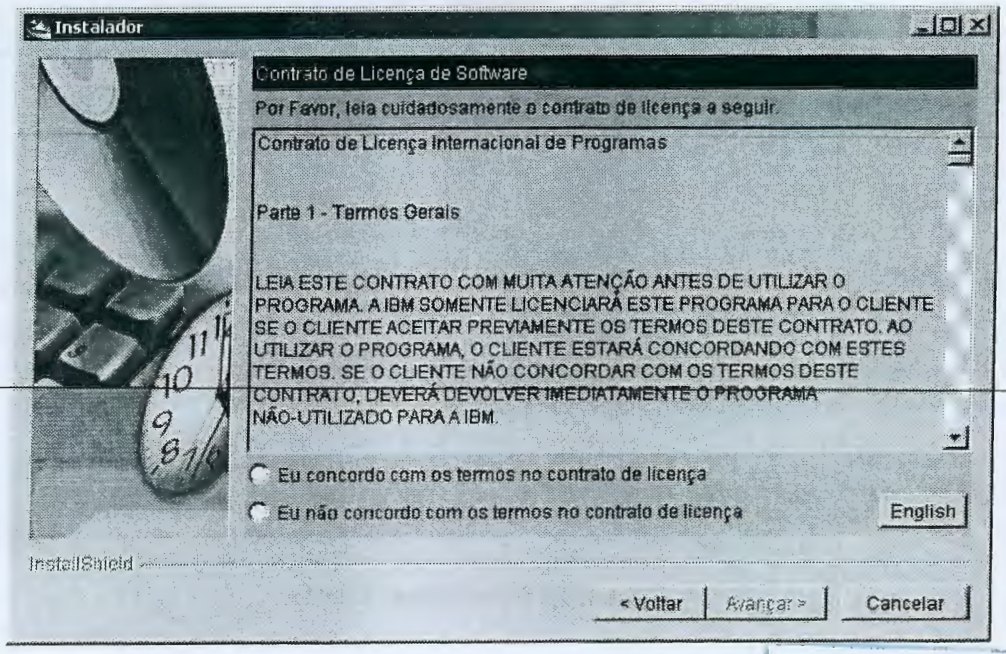


Figura 95. Painel Contrato de Licença de Software

8. Este painel de informação é exibido e informa que um componente do WebSphere está sendo implementado.

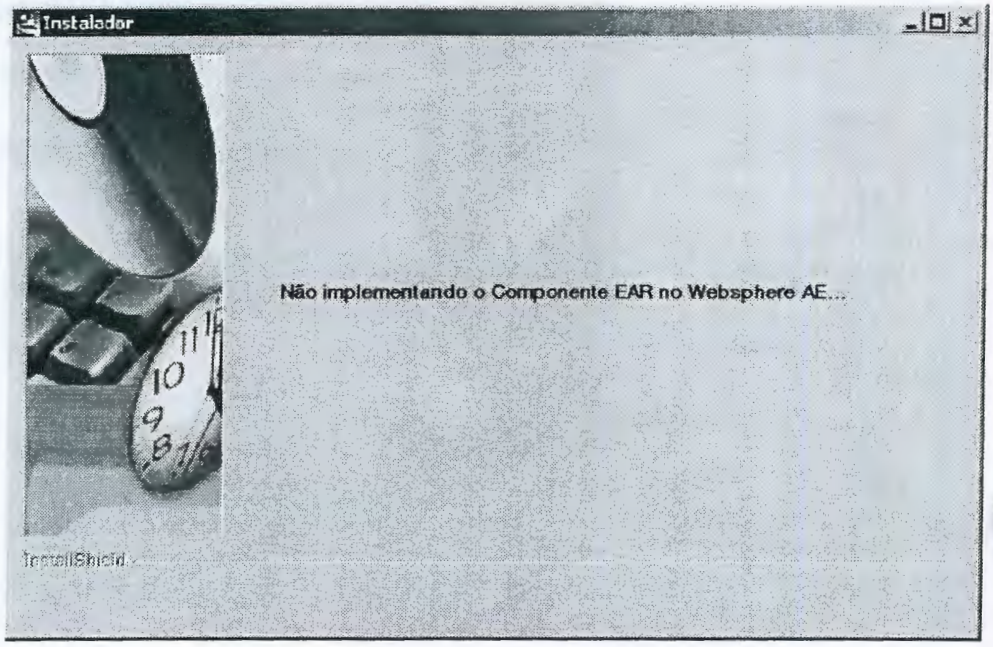


Figura 96. Painel Informações

9. O painel Número de Porta é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Clique em **Avançar** para continuar.

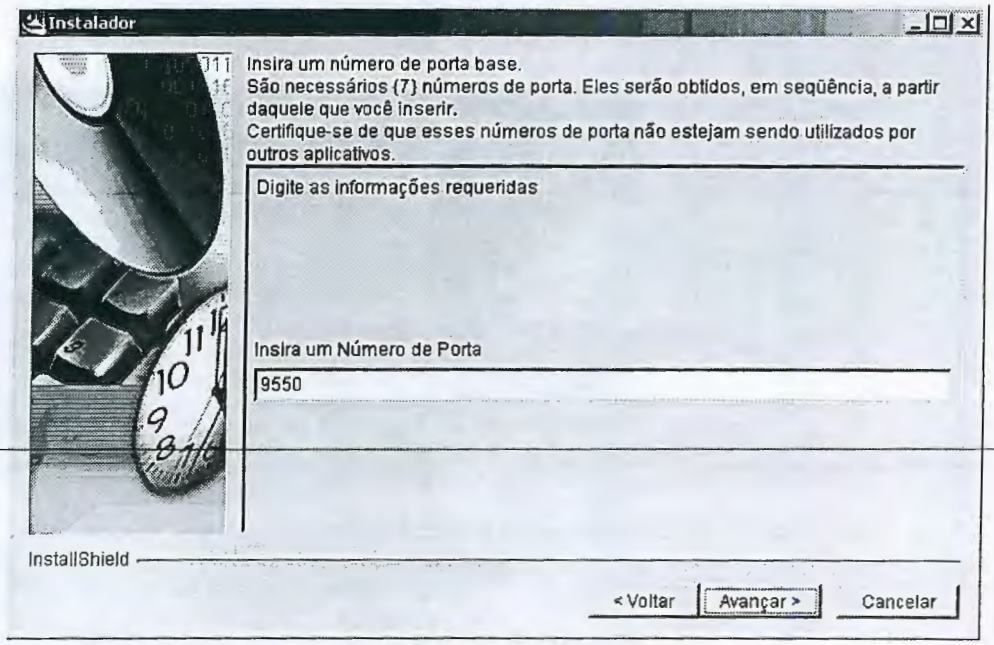


Figura 97. Painel Número de Porta

10. O painel ID do Usuário e Senha do Administrador DB2 é exibido. Para obter informações sobre esse ID de usuário do administrador do DB2, consulte a Tabela 12 na página 60. Insira o ID do administrador DB2 e insira a senha duas vezes. Certifique-se de que a senha não tenha expirado. Clique em **Avançar** para continuar.

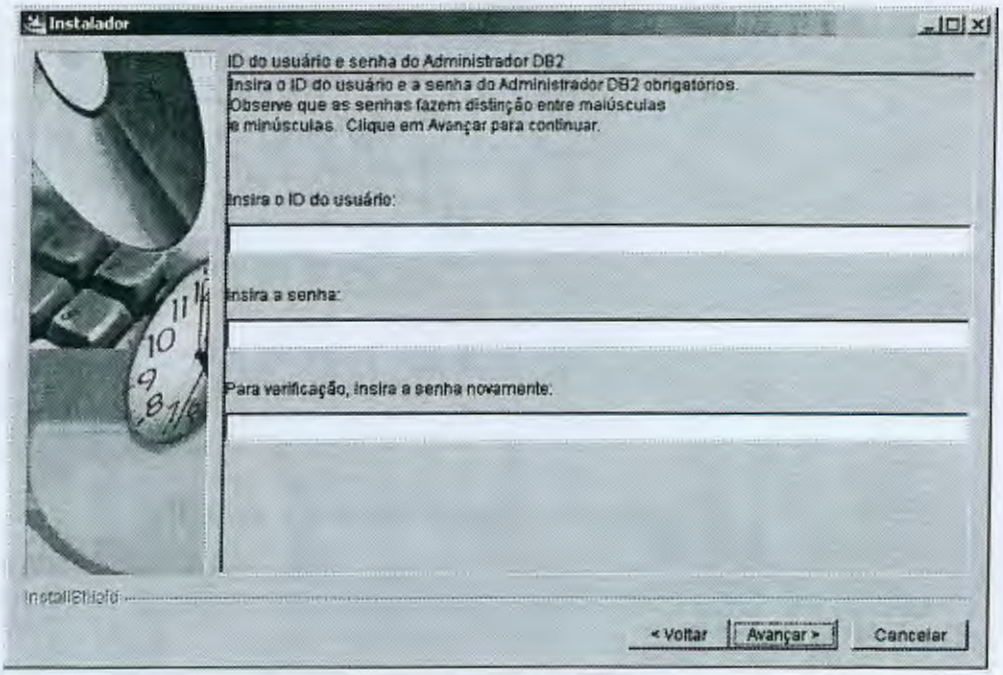


Figura 98. Painel ID do Usuário e Senha do Administrador DB2

11. O painel ID do Usuário e Senha DB2 é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior.

    Observe que o nome do banco de dados padrão para a versão 1.1 era **tivolsan**. Se esse não for o nome do seu banco de dados, insira o nome correto. Se o nome do banco de dados, o ID do usuário e a senha não forem os mesmos que da instalação anterior, os dados não serão migrados. Clique em **Avançar** para continuar.

    Nota: Se você estiver utilizando um ID de usuário e uma senha existentes, o programa de instalação não validará essa senha. Certifique-se de que o ID do usuário e a senha sejam válidos. Antes de continuar o programa de instalação, certifique-se também de que a senha não tenha expirado.

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 1570
3698
Doc.

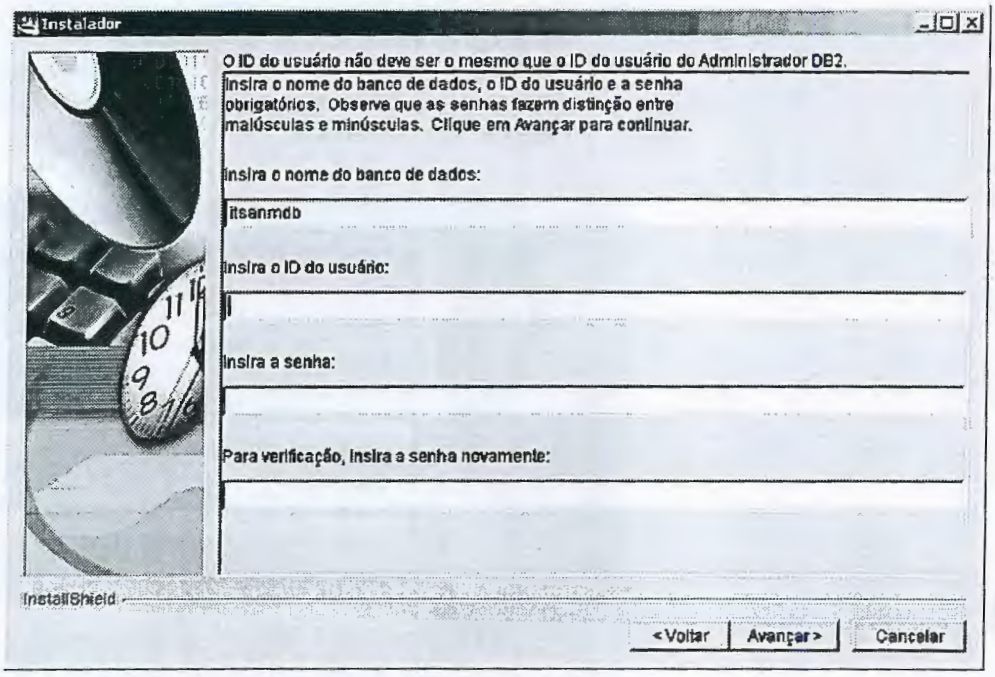


Figura 99. Painel ID do Usuário e Senha DB2

12. O ID do Usuário e a Senha para o painel WebSphere é exibido. Digite o ID do usuário e senha que você utilizou quando instalou o produto anterior.

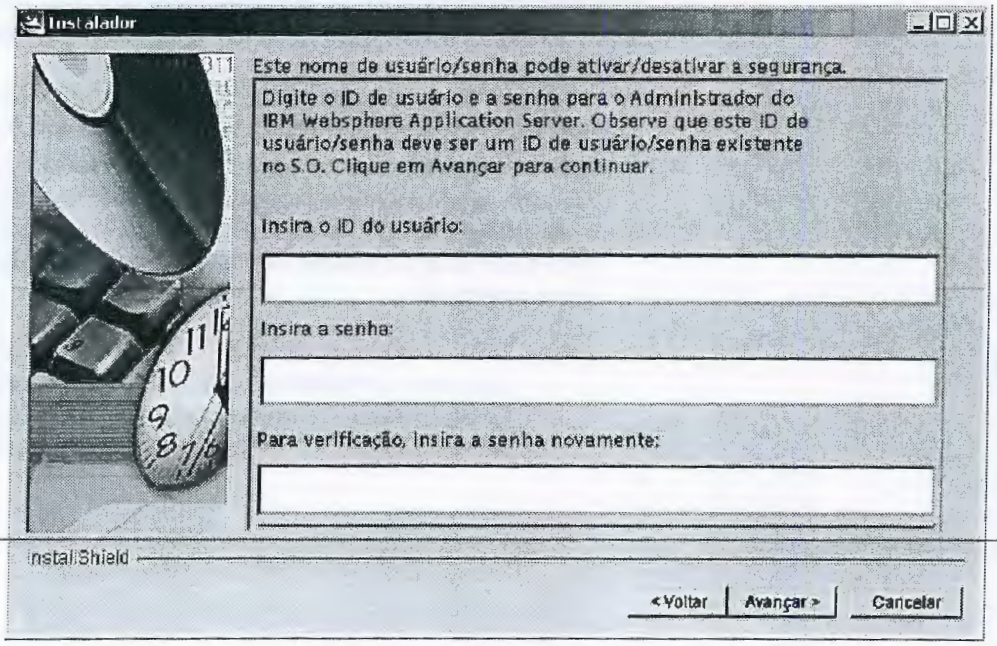


Figura 100. ID do Usuário e Senha para o Painel WebSphere

13. O painel Senha para Autenticação do Host é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Essa mesma senha deve ser utilizada para todos os hosts gerenciados e consoles remotos que se comunicam com este gerenciador. Para obter

informações sobre essa senha, consulte a Tabela 12 na página 60. Clique em **Avançar** para continuar.

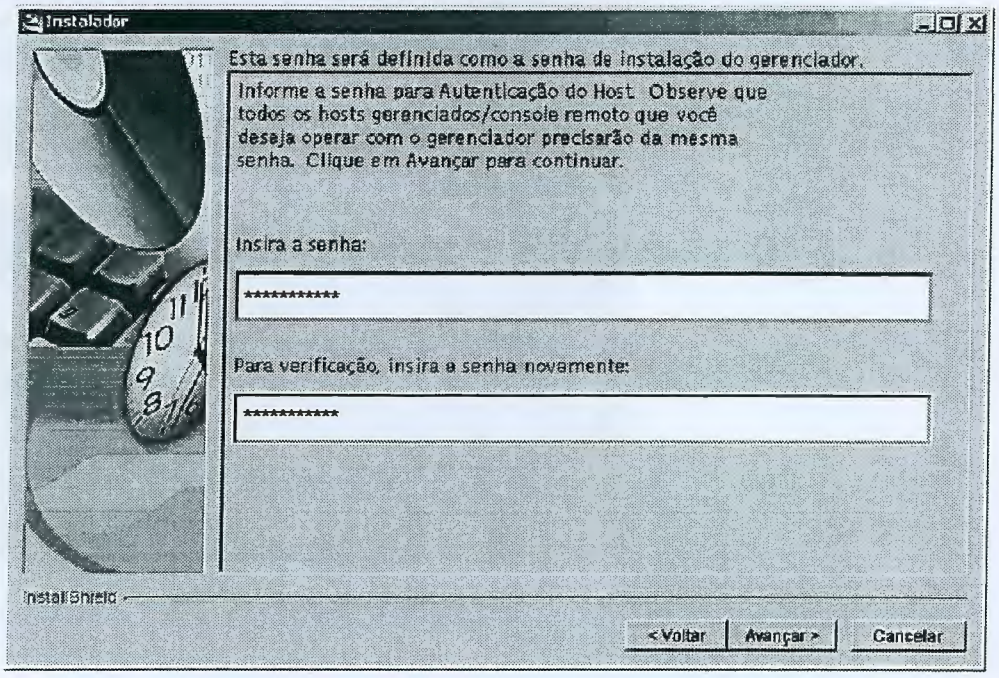


Figura 101. Painel Senha para Autenticação do Host

14. O painel Senha do Tivoli NetView é exibido. Para obter informações sobre o ID do usuário e a senha, consulte a Tabela 12 na página 60. Digite a mesma senha que você utilizou quando instalou o produto anterior. Clique em **Avançar** para continuar.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1571
Doc. 3698

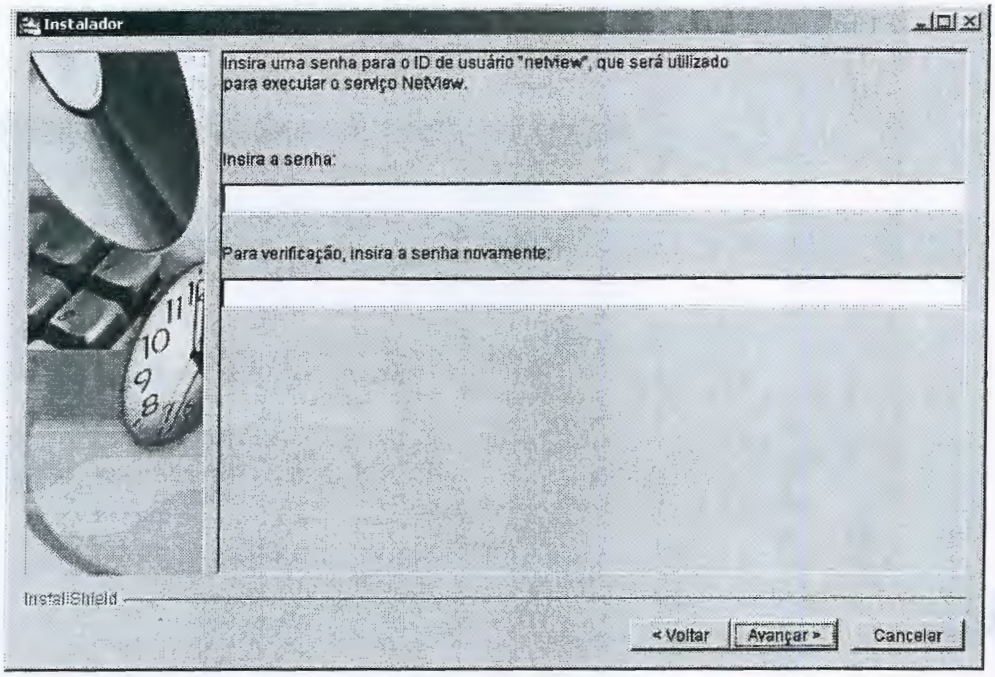


Figura 102. Painel Senha do Tivoli NetView

15. O painel Instalação do Tivoli Storage Area Network Manager é exibido. Clique em **Avançar** para continuar.

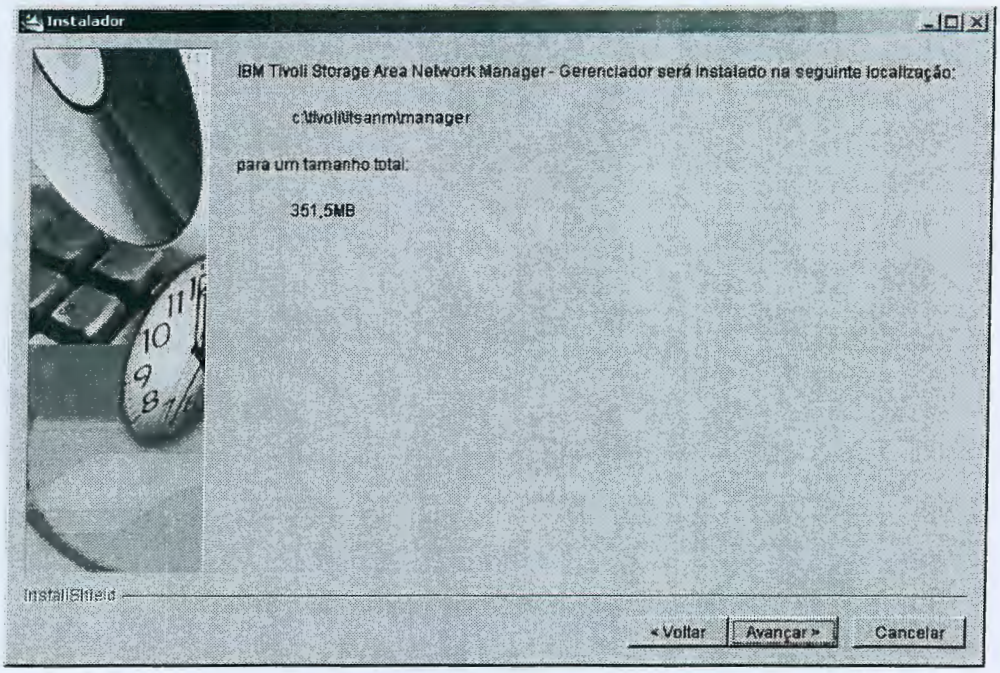


Figura 103. Painel Instalação do Tivoli Storage Area Network Manager

16. O painel Status do Tivoli Storage Area Network Manager é exibido. Esse procedimento pode levar aproximadamente de 15 a 20 minutos para ser concluído. Você verá outras janelas de prompt de comandos se abrindo e fechando conforme a instalação continua.
17. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido.

    Se a versão correta do Tivoli NetView tiver sido instalada antes da instalação do gerenciador, o botão **Concluir** será exibido. (O Tivoli NetView não será instalado com o gerenciador.) Você não verá o painel seguinte que solicita a reinicialização do sistema.

    Se o Tivoli NetView não tiver sido instalado anteriormente e for instalado com essa instalação do gerenciador, o painel seguinte será exibido. Esse painel solicita a reinicialização do sistema.

    Clique em **Concluir** ou **Avançar** para continuar.

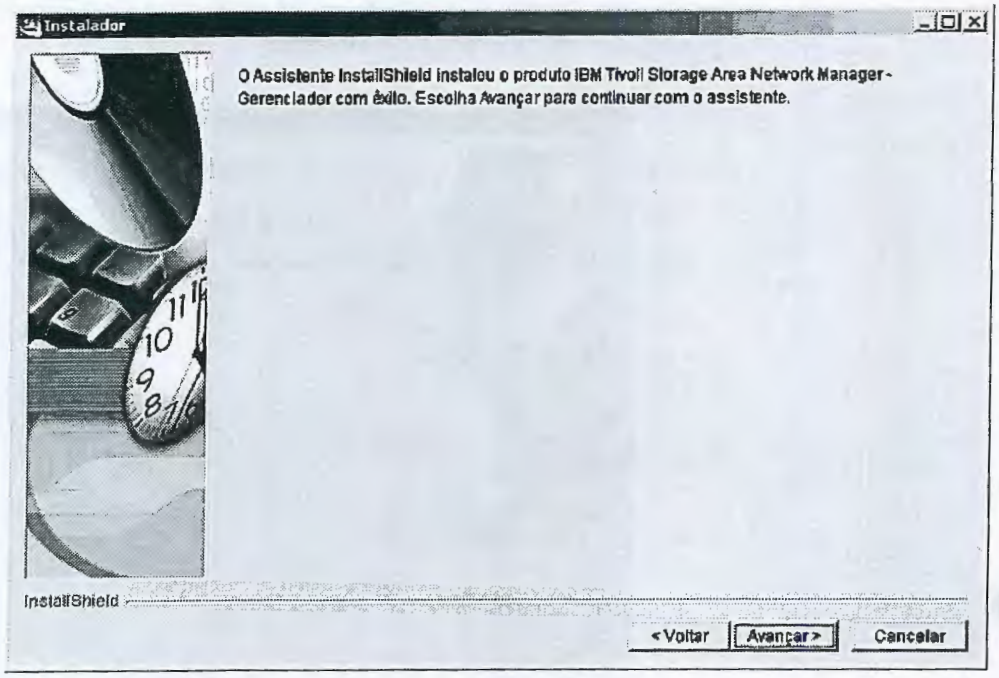


Figura 104. Painel Instalado com Êxito

18. O painel Instalação Concluída é exibido. Para iniciar o computador novamente, clique em **Sim, reinicialize meu sistema.** Clique em **Concluir** para concluir a instalação.

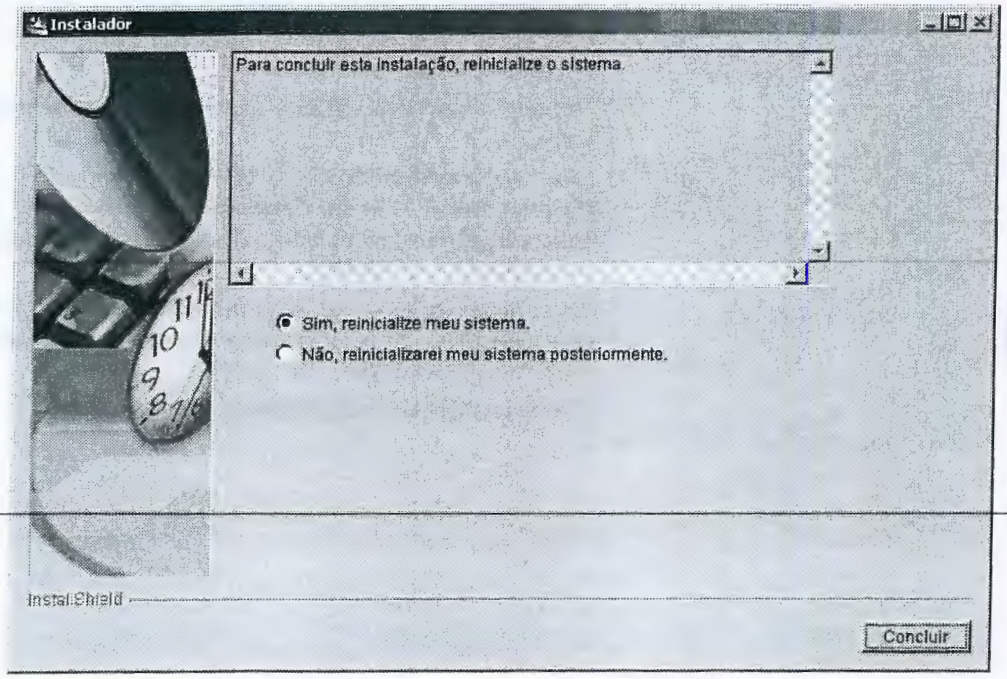


Figura 105. Painel Instalação Concluída

19. Depois de iniciar novamente o sistema, o serviço do Tivoli Storage Area Network Manager será automaticamente iniciado.

1015
A

Fazendo o Upgrade do Console Remoto

Siga estas etapas para fazer o upgrade do console remoto:

1. Certifique-se de que os seguintes aplicativos estejam encerrados:
   - Web Console
   - Web Console Security
   - MIB Loader
   - MIB Browser
   - Netmon Seed Editor
   - Tivoli Event Console Adaptor Configurator
2. Insira o CD do Tivoli Storage Area Network Manager Manager and Remote Console na unidade de disco de CD–ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD–ROM do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **launch.exe**. O painel Ativar é exibido. Selecione **Remote Console**. Clique em **Avançar** para continuar.

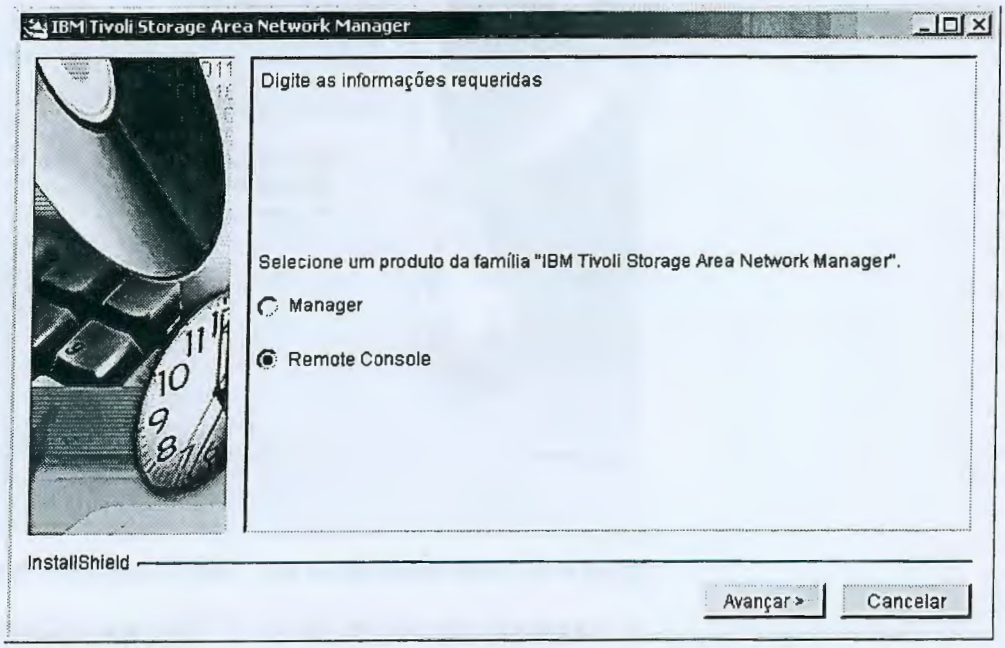


Figura 106. Painel Ativar

3. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para fazer o upgrade desse produto.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3698
Doc

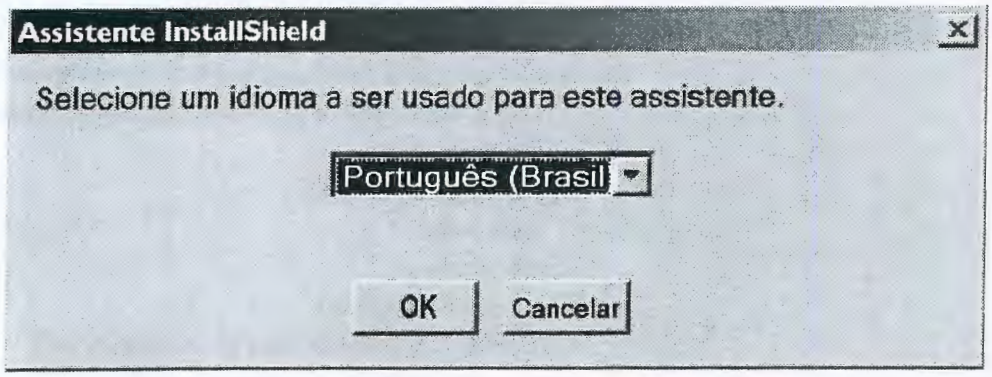


Figura 107. Painel Selecione um Idioma

4. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

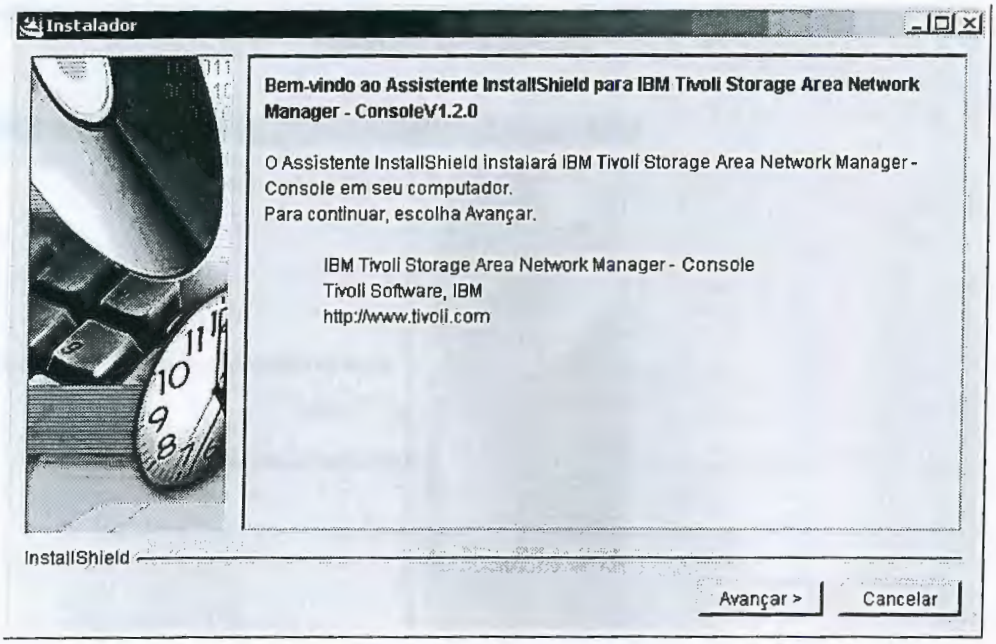


Figura 108. Painel Bem-vindo ao IBM Tivoli Storage Area Network Manager

5. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença.** Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o IBM Tivoli Storage Area Network Manager.

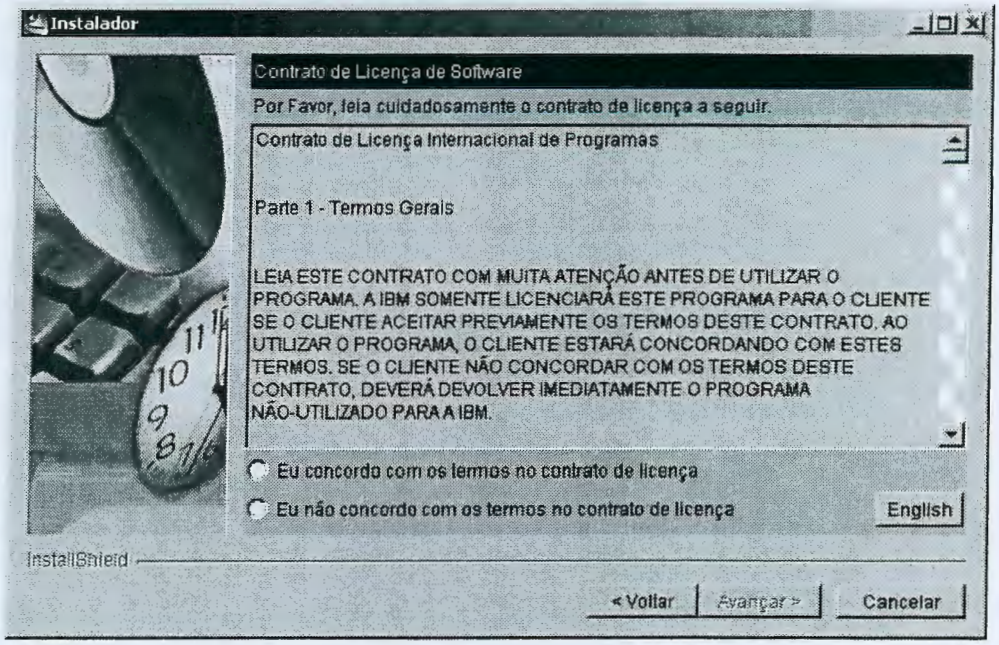


Figura 109. Painel Contrato de Licença de Software

6. O painel Informações sobre o Gerenciador é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Clique em **Avançar** para continuar.

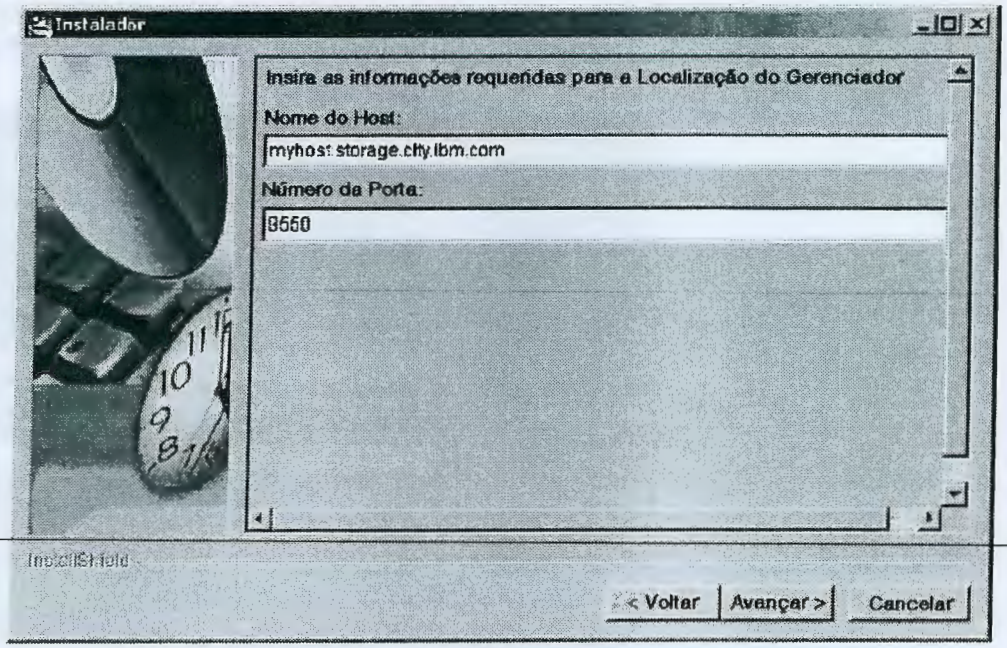


Figura 110. Painel Informações sobre o Gerenciador

7. O painel Número de Porta é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Para obter informações sobre números de porta, consulte a Tabela 7 na página 20. Clique em **Avançar** para continuar.

RQS nº 03/200
CPMI
Fls Nº 1574
Doc 3698

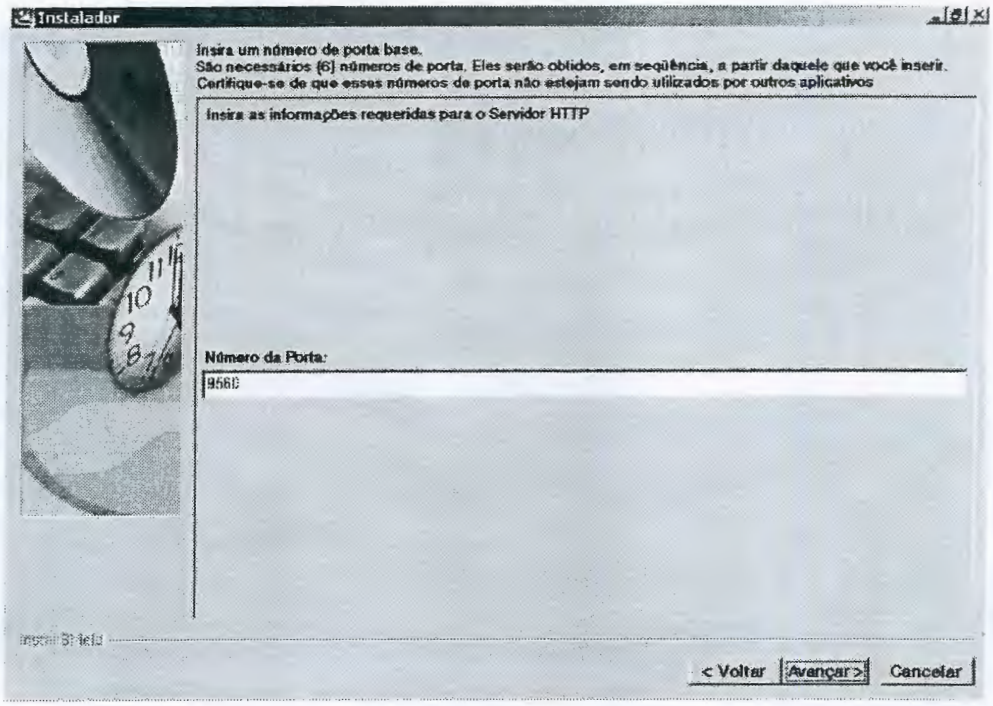


Figura 111. Painel Número de Porta

8. O painel Senha para Autenticação do Host é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Essa senha deve utilizar a mesma senha do gerenciador com o qual este console remoto se comunica. Para obter informações sobre essa senha, consulte a Tabela 12 na página 60. Clique em **Avançar** para continuar.

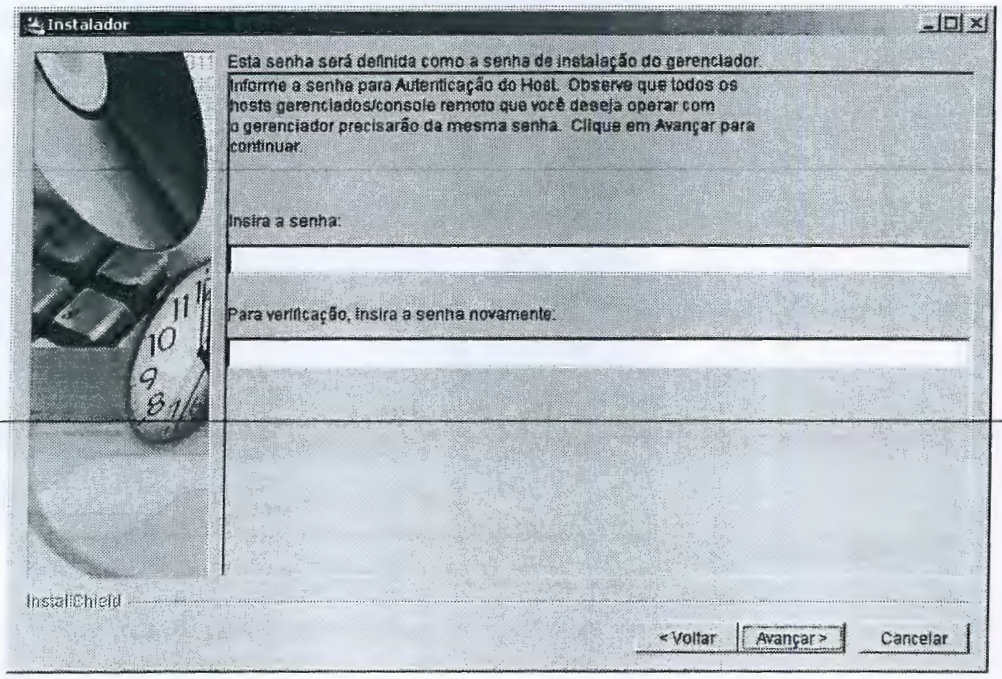


Figura 112. Painel Senha para Autenticação do Host

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1575
Doc 3698

9. O painel Senha do Tivoli NetView é exibido. Para obter informações sobre o ID do usuário e a senha, consulte a Tabela 12 na página 60. Insira a senha duas vezes. Clique em **Avançar** para continuar.

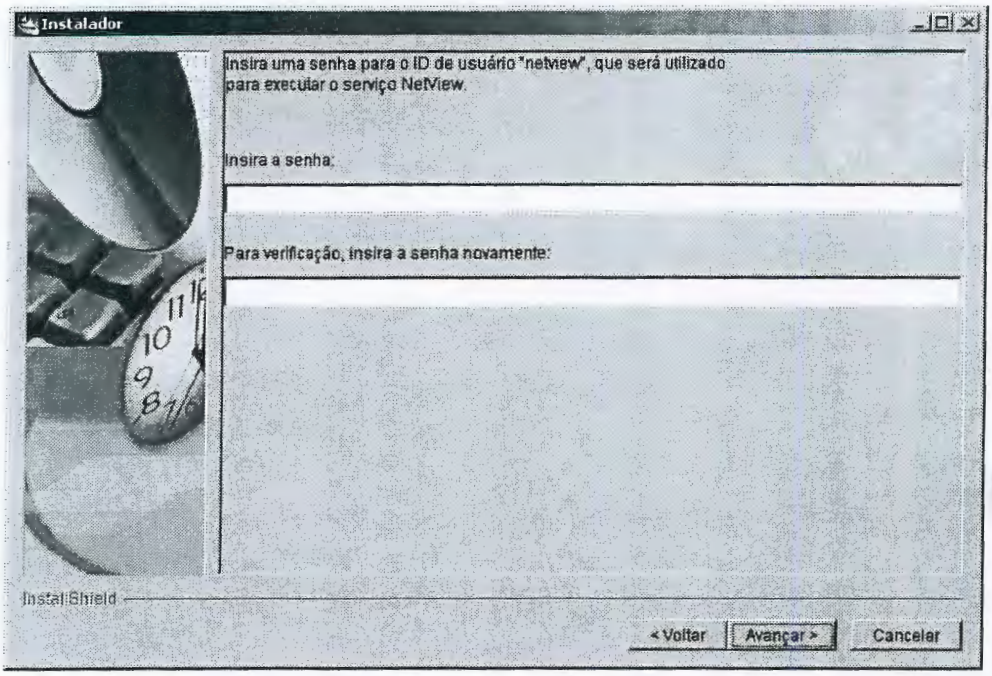


Figura 113. Painel Senha do Tivoli NetView

10. O painel Confirmação da Instalação é exibido. Confirme se o diretório especificado é o local em que você deseja instalar o console. Clique em **Avançar** para continuar.

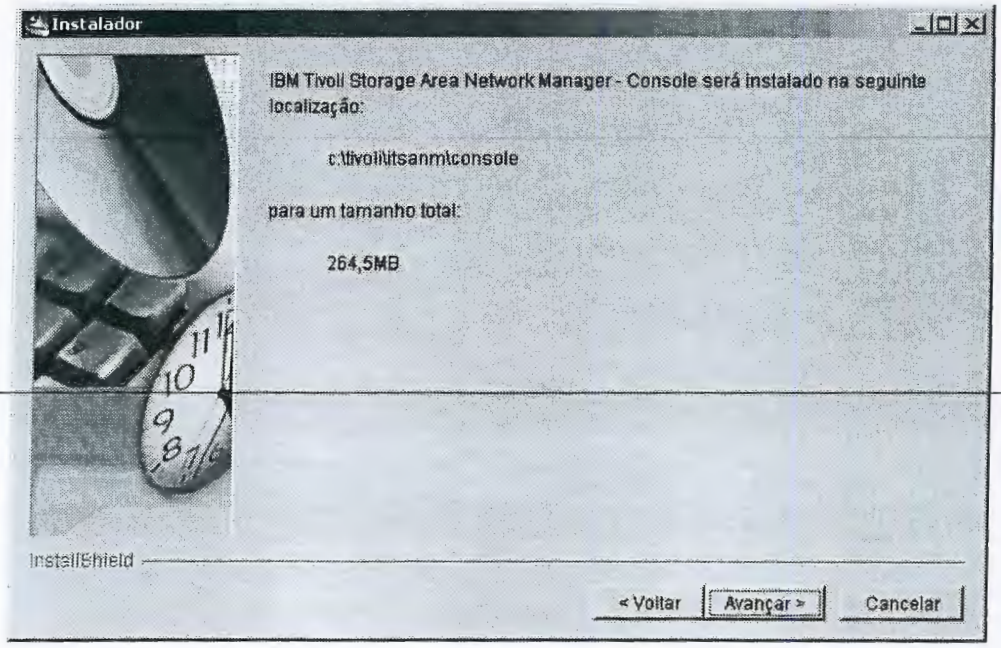


Figura 114. Painel Confirmação da Instalação

11. O painel Status é exibido. Esse procedimento demorará aproximadamente de 15 a 20 minutos.
12. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido. Clique em **Avançar** para continuar.

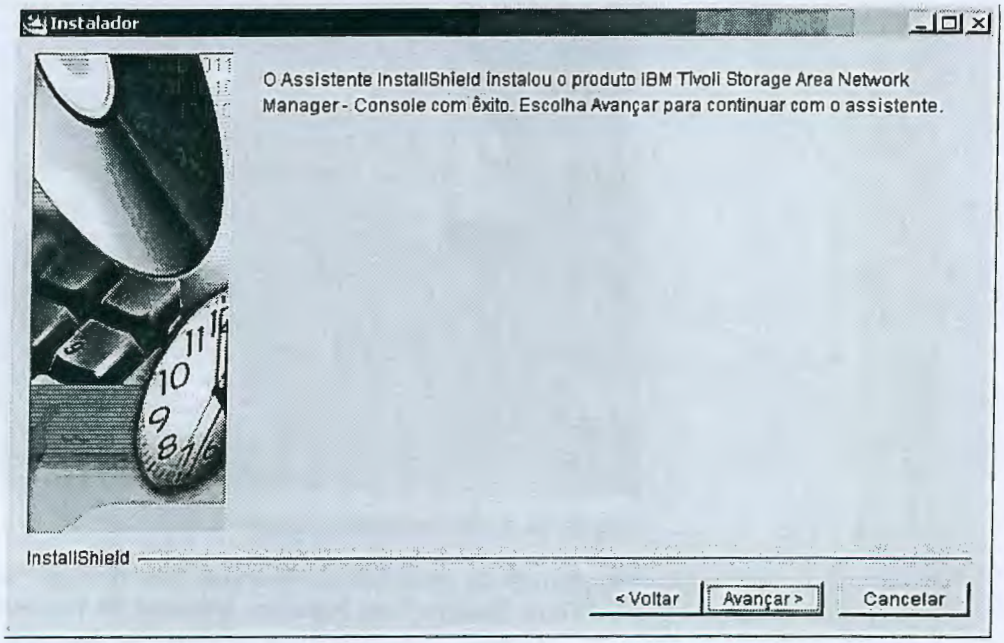


Figura 115. Painel Instalado com Êxito

13. O painel Instalação Concluída é exibido. Para iniciar o computador novamente, clique em **Sim, reinicialize meu sistema.** Clique em **Concluir** para concluir a instalação.

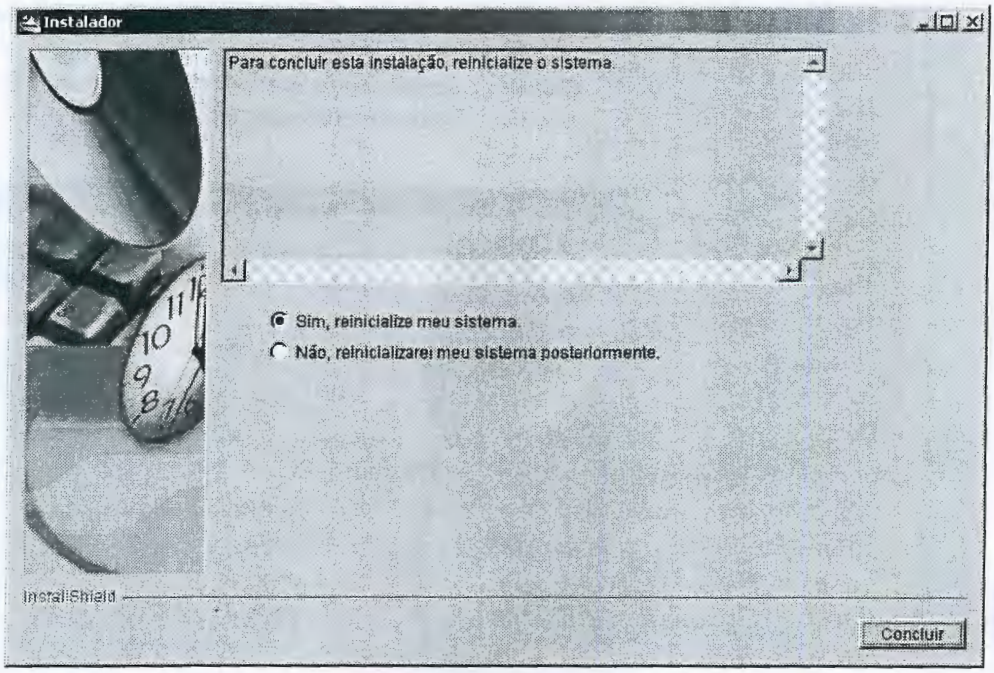


Figura 116. Painel Instalação Concluída

14. Depois de reinicializar o computador, verifique se o serviço do console do Tivoli Storage Area Network Manager foi iniciado. Clique no seguinte:

    `Iniciar → Configurações → Painel de controle → Ferramentas administrativas → Serviços (Serviços do NT) → Console do ITSANM`

Fazendo o Upgrade dos Agentes

Esta seção descreve como fazer o upgrade de agentes em plataformas diferentes.

Fazendo o Upgrade do Agente no Windows

Para fazer o upgrade do agente no Windows, siga estas etapas:

1. Insira o CD Tivoli Storage Area Network Manager Agents na unidade de disco de CD-ROM. Vá para o diretório do agente e dê um clique duplo em **setup.exe**.
2. O painel Selecione um Idioma é exibido. Selecione um idioma na lista drop down e clique em **OK**. Esse será o idioma utilizado para fazer o upgrade desse produto.

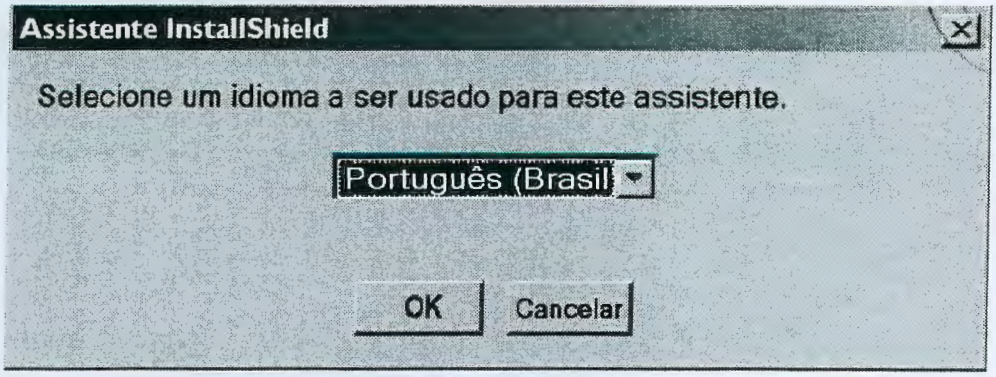


Figura 117. Painel Selecione um Idioma

3. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

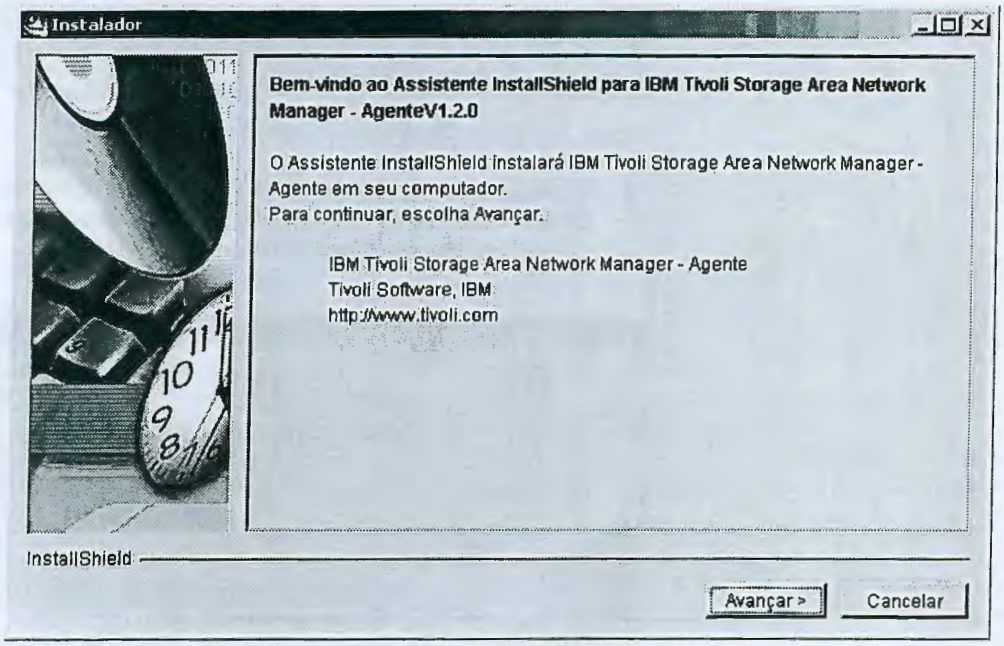


Figura 118. Painel Bem-vindo ao Tivoli Storage Area Network Manager

4. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o agente do Tivoli Storage Area Network Manager.

RQS nº 03/20 CPMI - CORR
Fls Nº 1577
Doc. 3698

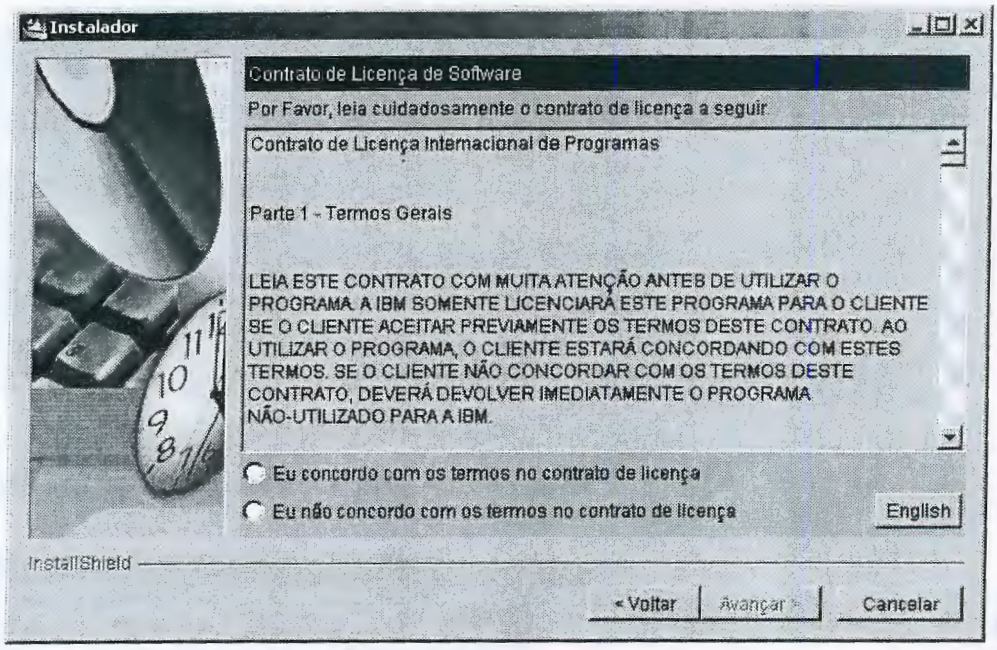


Figura 119. Painel Contrato de Licença

5. O painel Informações sobre o Gerenciador é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Clique em **Avançar** para continuar.

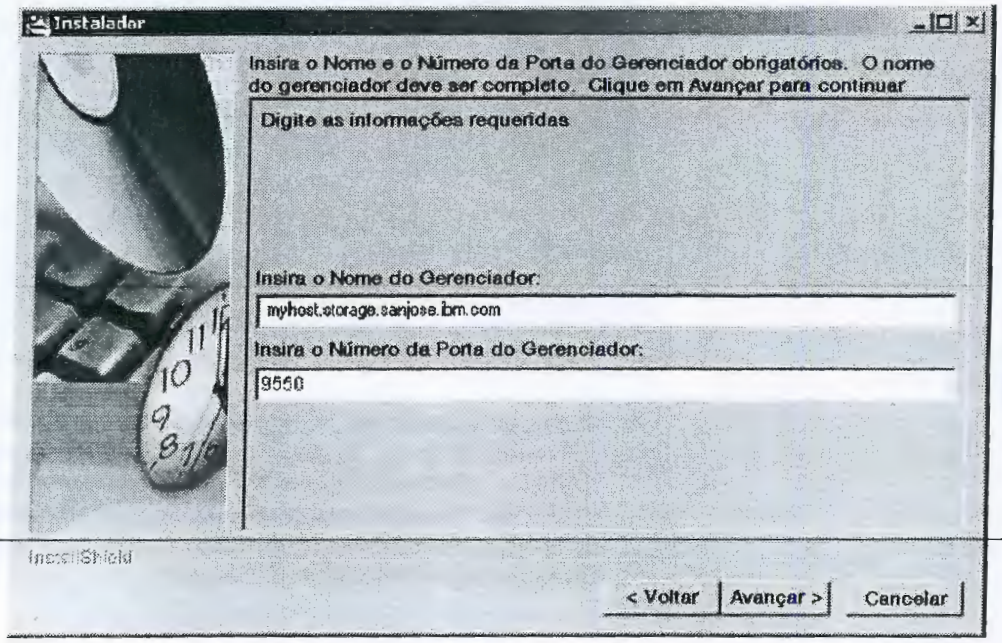


Figura 120. Painel Informações sobre o Gerenciador

6. O painel Número de Porta é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Clique em **Avançar** para continuar.

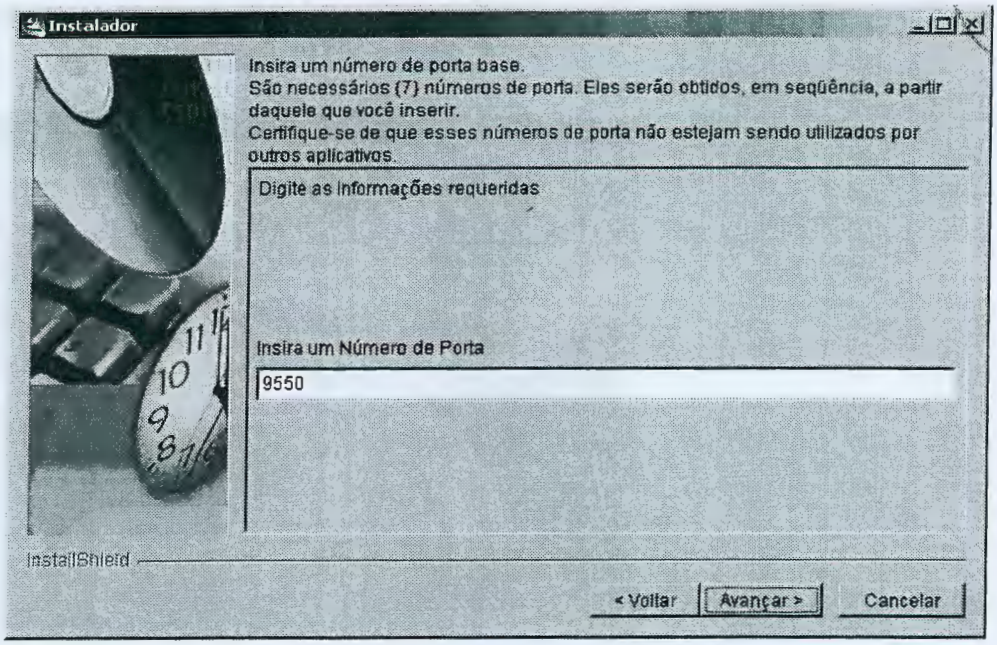


Figura 121. Painel Número de Porta

7. O painel Senha para Autenticação do Host é exibido. Este painel utiliza as mesmas informações que você forneceu quando instalou o produto anterior. Essa senha deve ser a mesma senha do gerenciador com o qual este host gerenciado se comunica. Para obter informações sobre essa senha, consulte a Tabela 12 na página 60. Clique em **Avançar** para continuar.

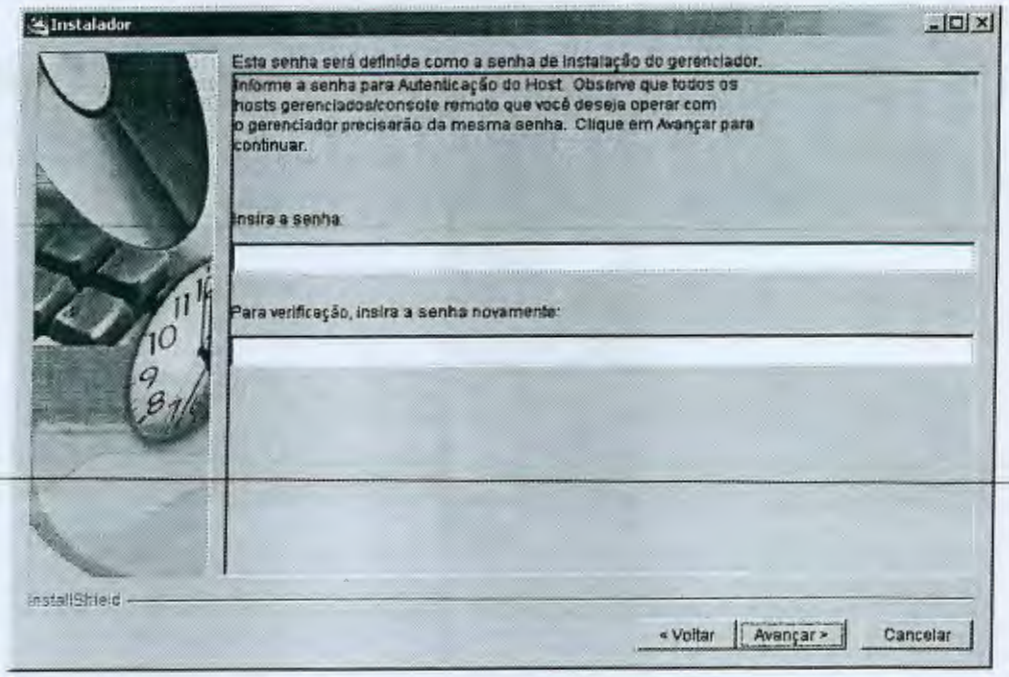


Figura 122. Painel Senha para Autenticação do Host

8. O painel Confirmação é exibido. Clique em **Avançar** para concluir.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1598
Nº Doc. 3698

Nota: Nos sistemas UNIX, o caminho do diretório é /tivoli/itsrm/agent. Observe que o caminho do diretório padrão para a versão 1.1.0 ou 1.1.1 era c:\tivoli\itsrm\agent.

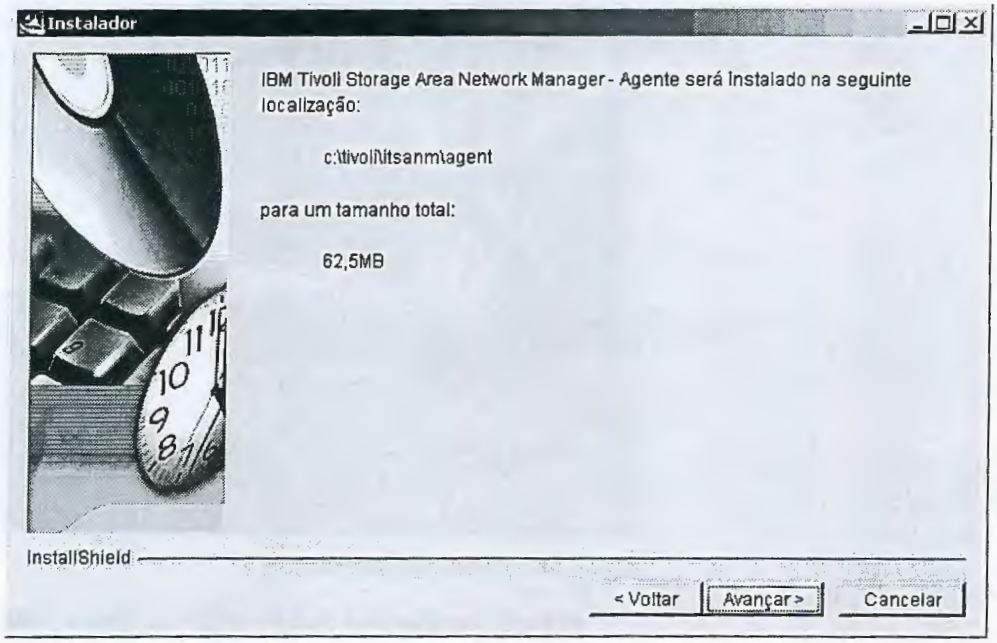


Figura 123. Painel Confirmação

9. O painel Status é exibido.
10. Quando a instalação estiver concluída, o painel Instalado com Êxito será exibido. Clique em **Concluir** para concluir a instalação.

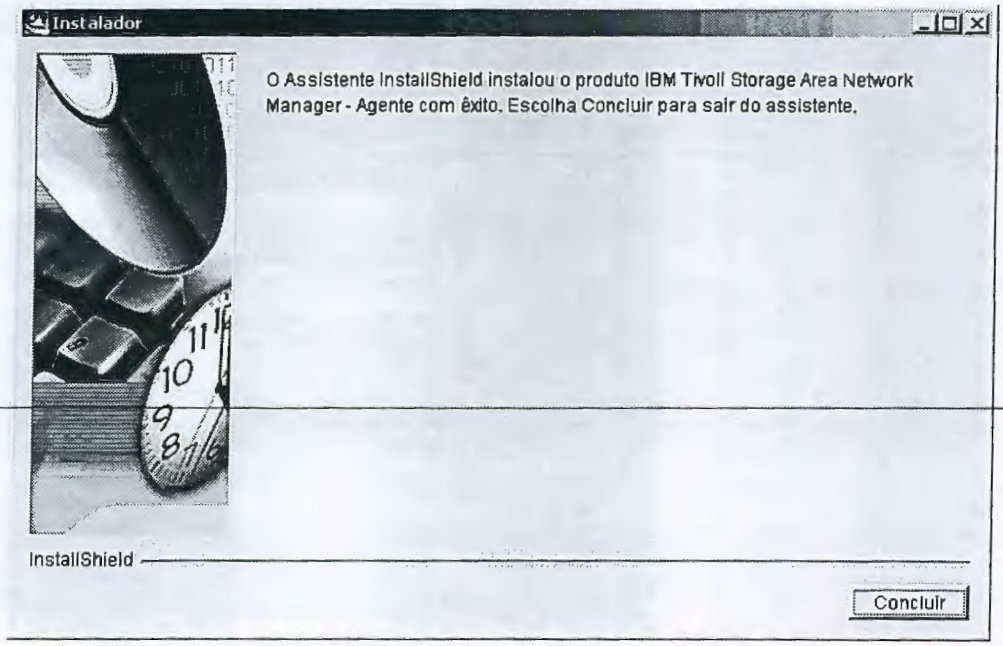


Figura 124. Painel Instalado com Êxito

11. O serviço do agente é automaticamente iniciado após a instalação.

Fazendo o Upgrade do Agente no AIX

Você deve ter autoridade root para fazer o upgrade do agente. Siga estas instruções para fazer o upgrade do agente do Tivoli Storage Area Network Manager:

1. Insira o CD do Agente IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
2. Utilize os comandos a seguir para determinar o diretório de montagem e executar o script de instalação. O script de upgrade da instalação está localizado no diretório do **agente**. Execute estes comandos:

```
mkdir /cdrom
mount -v'cdrfs' -r'' /dev/cd0 /cdrom
cd /cdrom/agent
./setup.aix
```

3. Siga as orientações nos painéis de instalação, começando com a etapa 2 na página 146.
4. O serviço do agente é automaticamente iniciado após a instalação.

Fazendo o Upgrade do Agente no Solaris

Você deve ter autoridade root para fazer o upgrade do agente. Siga estas instruções para fazer o upgrade do agente do Tivoli Storage Area Network Manager:

1. Insira o CD do Agente IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
2. A unidade deve ser montada manualmente. O script de upgrade da instalação está localizado no diretório do **agente**. Utilize estes comandos para determinar o diretório de montagem (por exemplo, `/cdrom/agent`) e executar o script de instalação:

```
df -k          (para procurar sistema montado)
  cd /cdrom/agent
  ./setup.sol       (para o Solaris)
```

3. Siga as orientações nos painéis de instalação, começando com a etapa 2 na página 146.
4. O serviço do agente é automaticamente iniciado após a instalação.

Capítulo 11. Instalando o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager

O Pacote de Idiomas permite visualizar mensagens, ajuda on-line e textos em um idioma diferente do inglês. Antes de instalar o Pacote de Idiomas, é necessário instalar o IBM Tivoli Storage Area Network Manager. O Pacote de Idiomas requer 40 MB de espaço em disco temporário para cada componente: o gerenciador, o host gerenciado e o console remoto.

Esta seção fornece informações sobre os seguintes itens:

Item	Consulte
Como instalar o Pacote de Idiomas no gerenciador do Windows	"Instalando o Pacote de Idiomas no Gerenciador do Windows"
Como instalar o Pacote de Idiomas no gerenciador do Windows	"Instalando o Pacote de Idiomas no Gerenciador do AIX" na página 162
Como instalar o Pacote de Idiomas no console remoto	"Instalando o Pacote de Idiomas no Console Remoto" na página 163
Como instalar o Pacote de Idiomas no host gerenciado	"Instalando o Pacote de Idiomas no Host Gerenciado" na página 163
Como remover a instalação do Pacote de Idiomas	"Removendo a Instalação do Pacote de Idiomas" na página 165

Instalando o Pacote de Idiomas no Gerenciador do Windows

O Pacote de Idiomas também instala o Kit de Idiomas do Tivoli NetView.

Para instalar o Pacote de Idiomas, siga estas etapas:

1. Pare o serviço do gerenciador. Para parar o serviço do gerenciador, clique em:

   `Iniciar -> Configurações -> Painel de Controle -> Ferramentas Administrativas -> Serviços`

   O painel Serviços é exibido. Dê um clique com o botão direito do mouse em **IBM WebSphere Application Server V5 – ITSANM-Manager**. Clique em **Parar**.
2. Pare o console. No Painel de serviços, clique com o botão direito do mouse em **ITSANM – Console**. Clique em **Parar**. Pare também o serviço do Tivoli NetView.
3. Insira o CD do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager na unidade de CD-ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se o programa não se iniciar automaticamente, abra o Windows Explorer e vá para a unidade de disco de CD-ROM do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager.
4. No diretório da unidade de CD-ROM, dê um clique duplo em **setup.exe**.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1580
3698
Doc

5. O painel Selecione um Idioma é exibido. Selecione um idioma na caixa drop down e clique em **OK**. Esse será o idioma utilizado para a instalação deste produto.

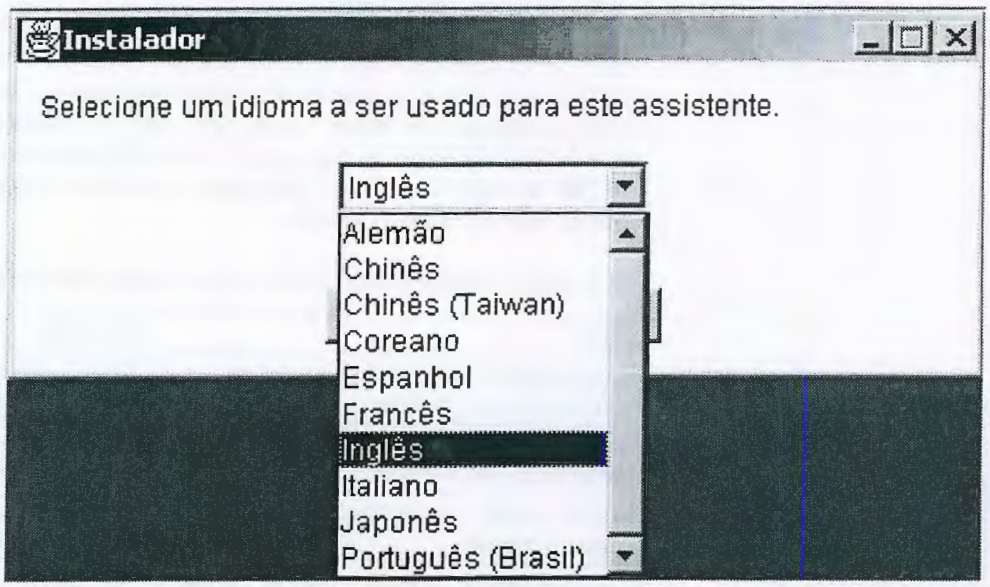


Figura 125. Painel Selecione um Idioma

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

10144
A.

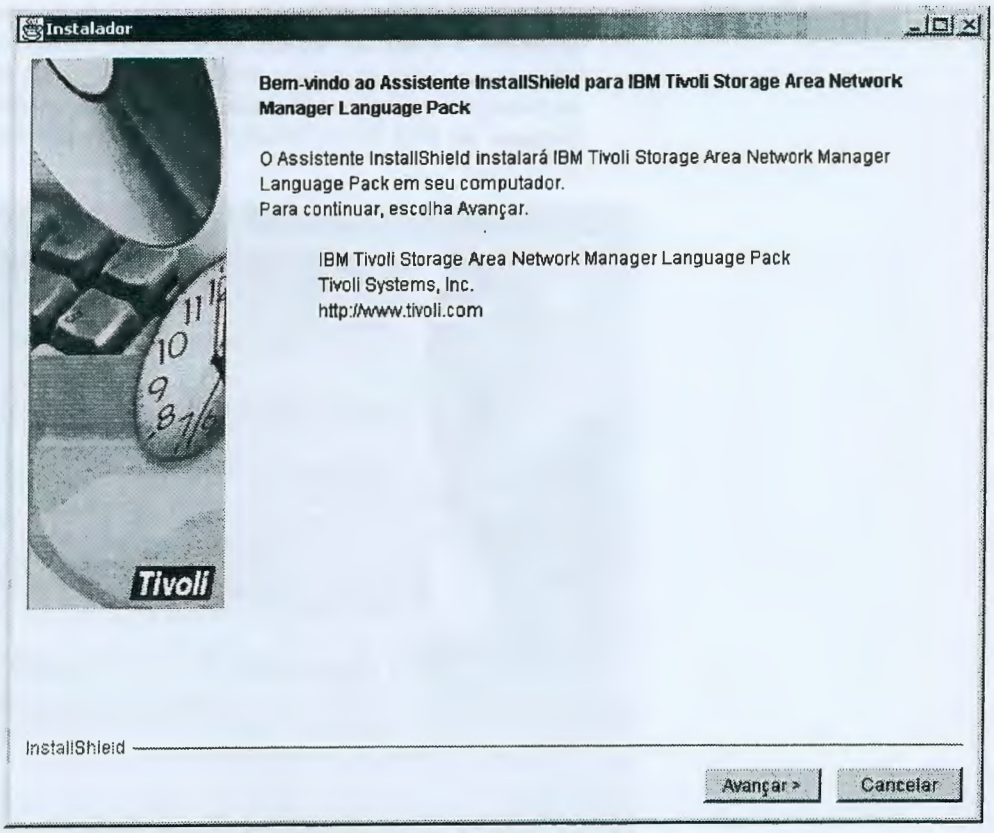


Figura 126. Painel Bem-vindo

ROS nº 032006 - CN
CPMI - CORREIOS
FLS Nº 1581
3698
DOC

7. O painel Contrato de Licença de Software é exibido. Leia os termos do contrato de licença. Se você concordar com os termos do contrato de licença, selecione o botão de opções **Eu aceito os termos no contrato de licença**. Clique em **Avançar** para continuar. Se você não aceitar os termos do contrato de licença, o programa de instalação será encerrado sem instalar o Pacote de Idiomas do IBM Tivoli Storage Area Network Manager.

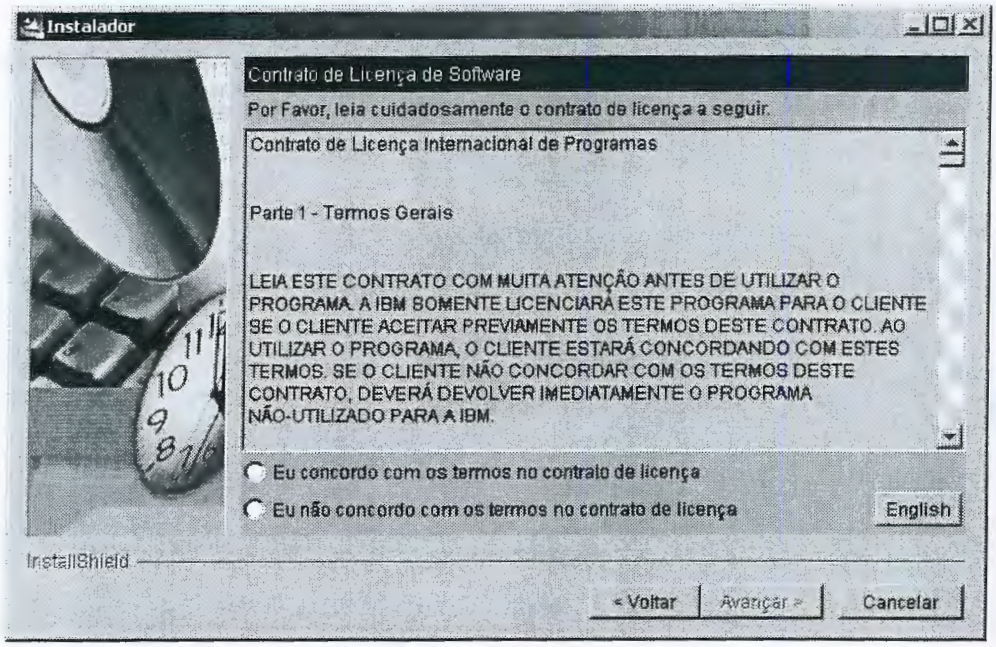


Figura 127. Painel Contrato de Licença de Software

8. O painel Nome do Diretório é exibido. Os nomes de diretório e caminho não devem conter espaços ou hifens. Insira um nome de diretório diferente ou aceite o nome de diretório padrão. O programa criará o nome do diretório padrão se ele ainda não existir. Clique em **Avançar** para continuar.

   Nota: O nome do caminho UNIX no painel é diferente do utilizado no Windows. Por exemplo, no UNIX, o nome do caminho seria /tivoli/itsanm/LangPacks.

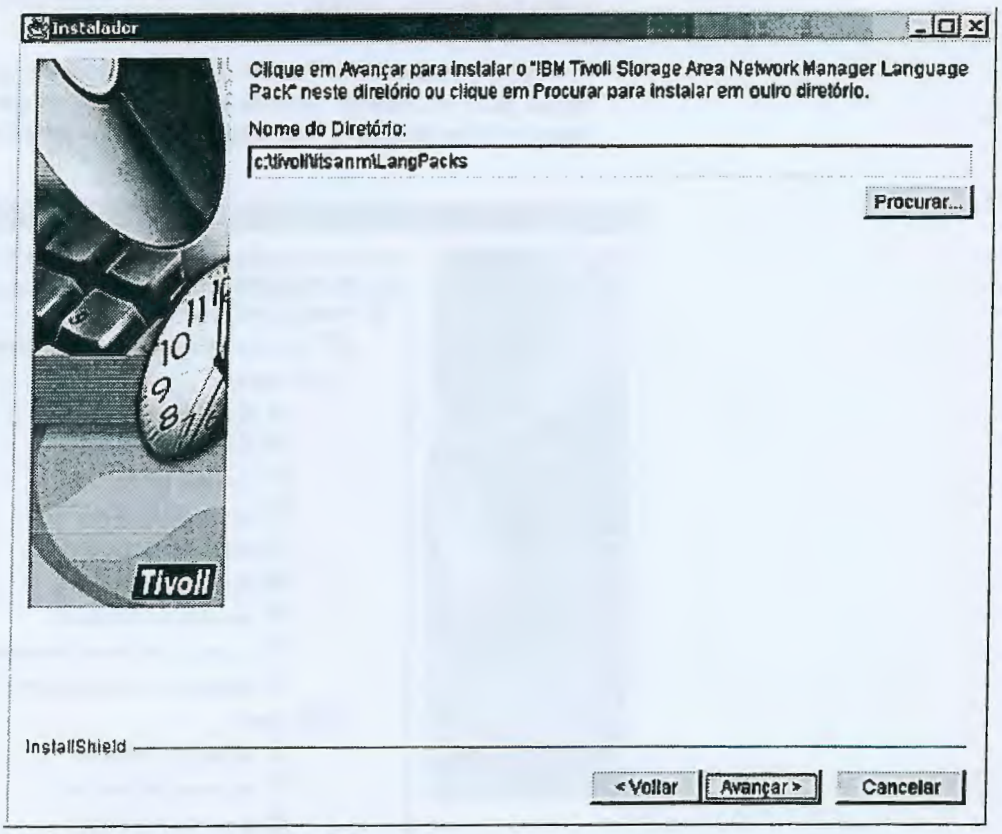


Figura 128. Painel Nome do Diretório

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1582
Doc. 3698

9. O painel Selecione os Recursos é exibido. As informações nesse painel são alteradas dependendo do componente que você está instalando e dos idiomas instalados no sistema.

   Se você estiver instalando o Pacote de Idiomas para o gerenciador, marque as caixas para o Gerenciador e os idiomas em que deseja exibir o IBM Tivoli Storage Area Network Manager.

   Se estiver instalando o Pacote de Idiomas para o host gerenciado, marque as caixas para o Agente e os idiomas em que deseja exibir o IBM Tivoli Storage Area Network Manager. Se você tiver um agente e o gerenciador na mesma máquina, poderá instalar o Pacote de Idiomas para os dois componentes ao mesmo tempo.

   Se estiver instalando o Pacote de Idiomas para o console remoto, marque as caixas para o Console Remoto e os idiomas em que deseja exibir o IBM Tivoli Storage Area Network Manager. Clique em **Avançar** para continuar.

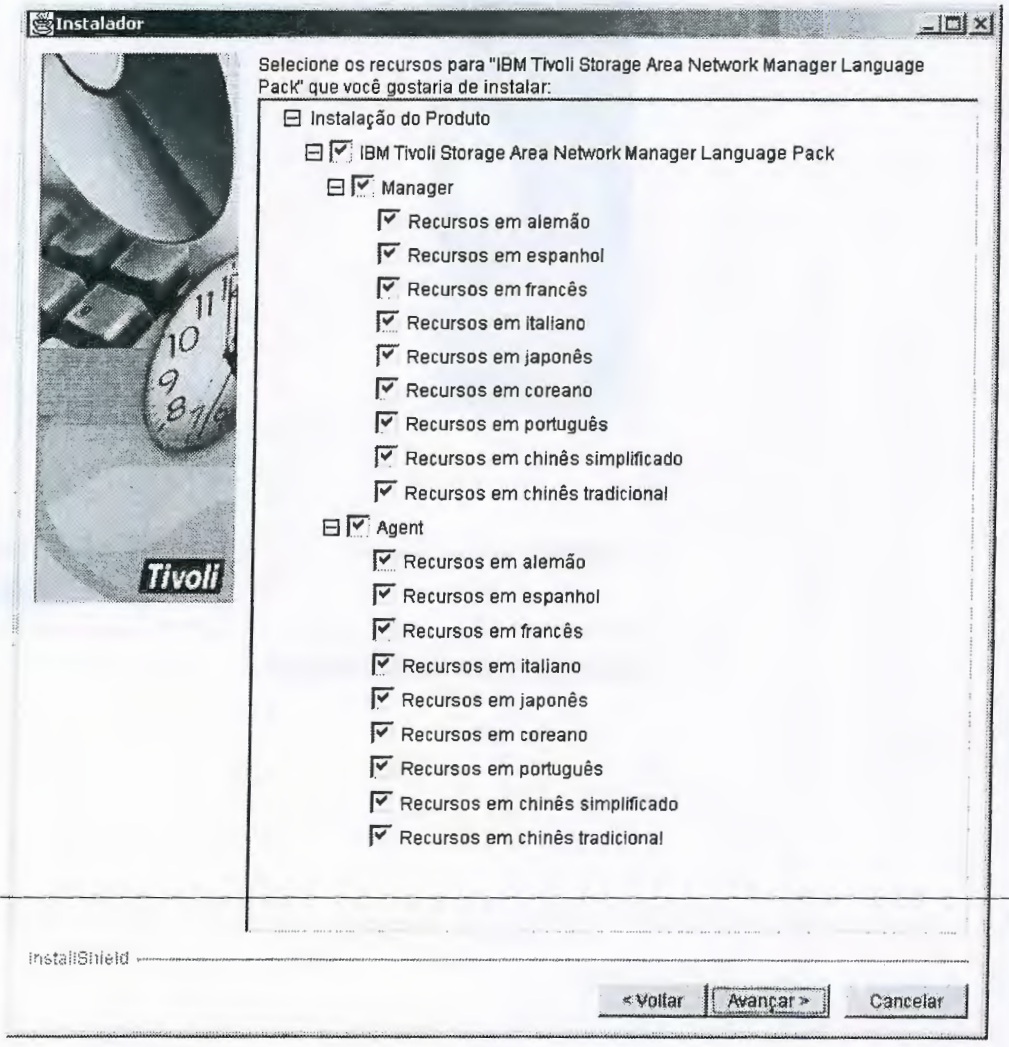


Figura 129. Painel Selecione os Recursos

10. O painel Idioma para o Tivoli NetView é exibido. Esse painel permite escolher o idioma no qual você deseja exibir as informações do Tivoli NetView. O Tivoli NetView somente é fornecido com os idiomas listados no painel. Selecione uma opção e clique em **Avançar** para continuar.

    Nota:

    - O IBM Tivoli Storage Area Network Manager *não* oferece suporte para o console da Web Tivoli NetView.
    - Este painel não aparece na instalação do Pacote de Idiomas para o gerenciador ou agentes do AIX.

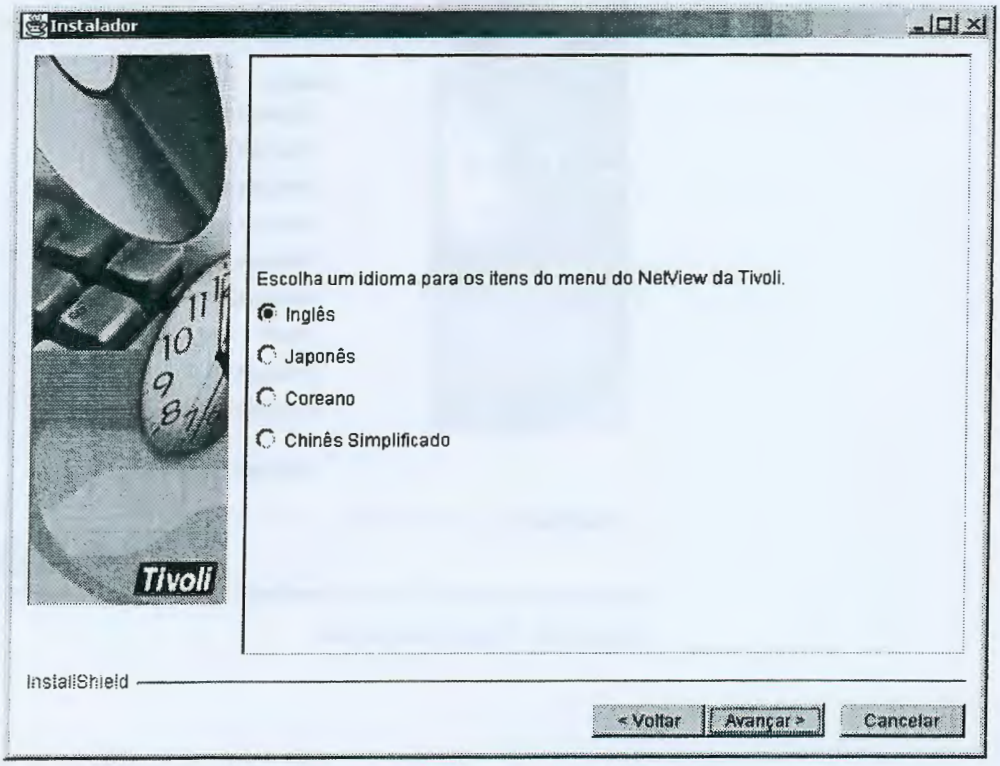


Figura 130. Painel Idioma para o Tivoli NetView

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1583
Doc. 3698

11. O painel Informações é exibido. Esse painel exibe suas opções de instalação. Revise essas informações e clique em **Avançar** para continuar.

Nota: Se você estiver instalando Pacote de Idiomas no UNIX, o caminho do diretório será diferente do Windows. Por exemplo, o caminho do diretório do UNIX seria /tivoli/itsanm/LangPacks.

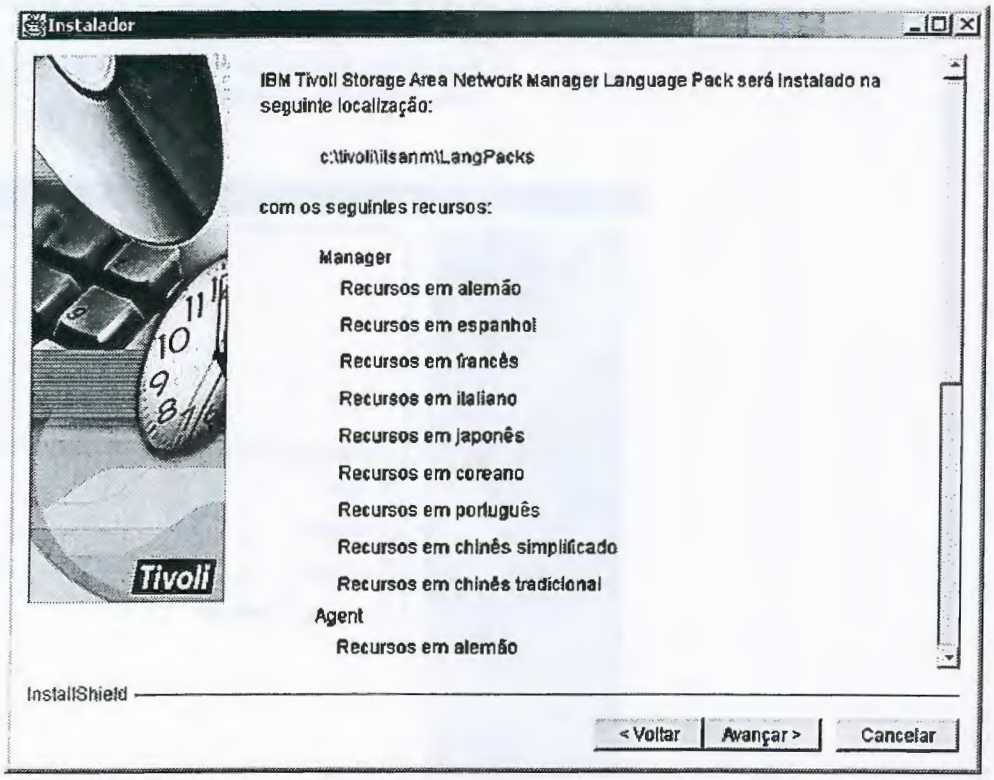


Figura 131. Painel Informações

12. O painel Status da Instalação é exibido. Depois de concluída a instalação, você verá o painel seguinte.

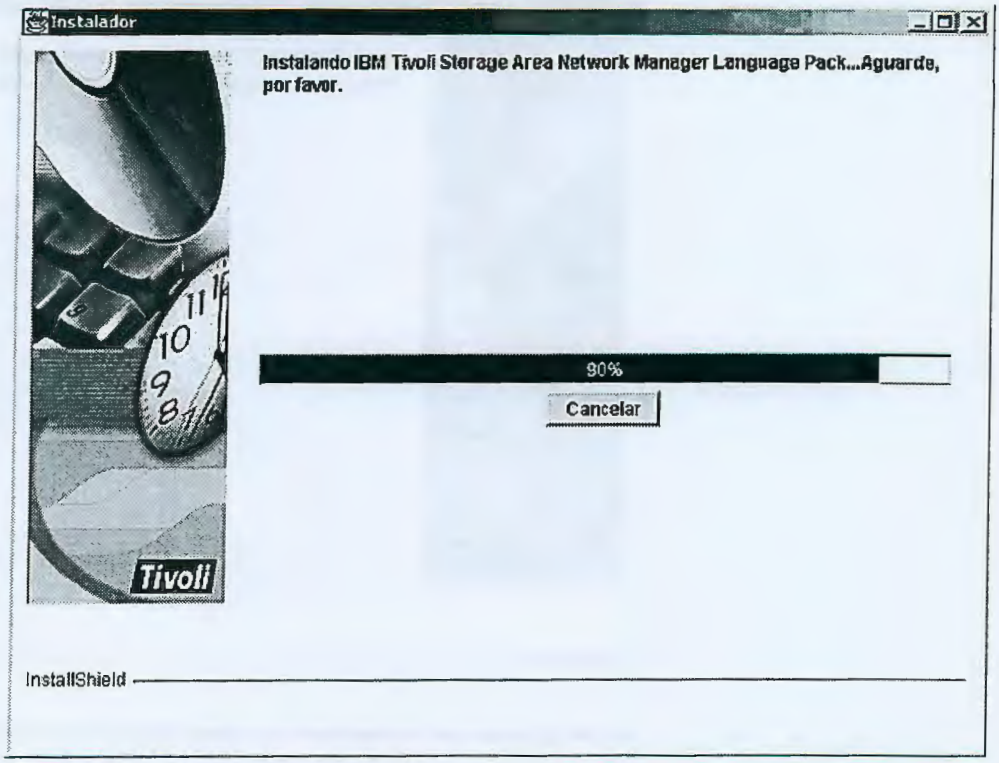


Figura 132. Painel Status da Instalação

13. O painel Instalado com Êxito é exibido. Clique em **Concluir** para concluir a instalação.

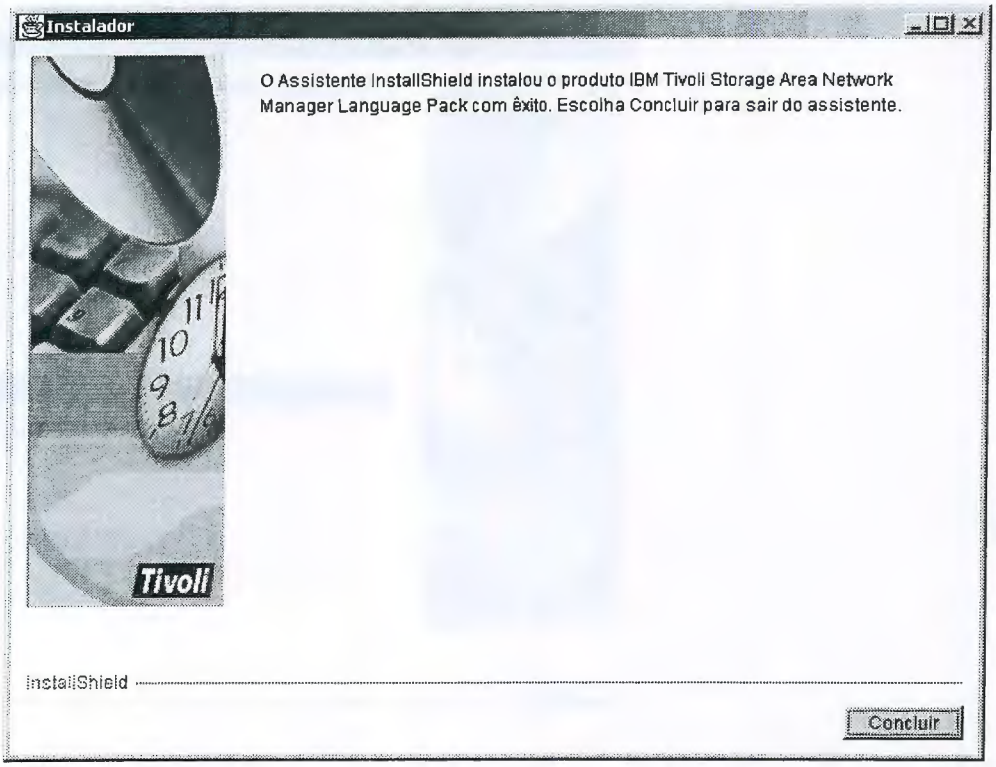


Figura 133. Painel Instalado com Êxito

14. Para o gerenciador do Windows, inicie novamente o ITSANM–Manager e o Tivoli NetView Service pelo painel Serviços do Windows.
15. Para o console remoto, inicie novamente o Serviço do Tivoli NetView e o Console do ITSANM. Na barra de ferramentas, clique no seguinte:

    `Iniciar → Configurações → Painel de Controle → Ferramentas Administrativas → Serviços (Serviços do NT) → Serviço do Tivoli NetView`

    Clique com o botão direito do mouse em **Serviço do Tivoli NetView** e, em seguida, clique em **Iniciar**. Faça o mesmo para o Console do ITSANM.
16. Para os hosts gerenciados, inicie novamente o Agente ITSANM. Para iniciar novamente os hosts gerenciados, consulte "Instalando o Pacote de Idiomas no Host Gerenciado" na página 163.

Instalando o Pacote de Idiomas no Gerenciador do AIX

Para instalar o Pacote de Idiomas, siga estas etapas:

1. Pare o serviço do gerenciador. Vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

   `/tivoli/itsanm/manager/bin/aix/stopSANM.sh`
2. Insira o CD do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
3. Utilize esses comandos para criar o diretório e determine o diretório de montagem. O comando também executa o script de instalação. O script de instalação está localizado no diretório **manager**. Execute estes comandos:

10136
A

```
mkdir /cdrom
mount -v'cdrfs' -r'' /dev/cd0 /cdrom
cd /cdrom/manager
./setup.aix
```

Observe que a opção –r é acompanhada de duas aspas.

4. Siga as orientações nos painéis de instalação, começando com a etapa 5 na página 154.
5. Inicie novamente o gerenciador. Para iniciar o gerenciador no AIX, vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

```
/tivoli/itsanm/manager/bin/aix/startSANM.sh
```

Instalando o Pacote de Idiomas no Console Remoto

Siga estas etapas para instalar o Pacote de Idiomas no console remoto:

1. Pare o console remoto e o Serviço do Tivoli NetView por meio do painel Serviços do Windows. Na barra de ferramentas, clique no seguinte:

   Iniciar → Configurações → Painel de Controle → Ferramentas Administrativas → Serviços (Serviços do NT) → Console do ITSANM

   Clique com o botão direito do mouse em **Console do ITSANM** e, em seguida, clique em **Parar**. Faça o mesmo para o Serviço do Tivoli NetView.
2. Insira o CD do Pacote de Idiomas do Tivoli Storage Area Network Manager na unidade de CD–ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD–ROM do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **setup.exe**.
3. Siga as orientações nos painéis de instalação, começando com a etapa 5 na página 154.

Instalando o Pacote de Idiomas no Host Gerenciado

Esta seção descreve como instalar o Pacote de Idiomas nos hosts gerenciados.

Instalando o Pacote de Idiomas no Windows

Siga estas etapas para instalar o Pacote de Idiomas no Windows:

1. Pare o serviço do agente. Para parar o serviço do agente, clique em:

   Iniciar → Configurações → Painel de Controle → Ferramentas Administrativas → Serviços

   O painel Serviços é exibido. Clique com o botão direito do mouse em **Agente ITSANM**. Clique em **Parar**.
2. Insira o CD do Pacote de Idiomas do Tivoli Storage Area Network Manager na unidade de CD–ROM. Se o autorun do Windows estiver ativado, o programa de instalação deverá ser iniciado automaticamente. Se isso não acontecer, abra o Windows Explorer e acesse a unidade de CD–ROM do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager. Dê um clique duplo em **setup.exe**.
3. Siga as orientações nos painéis de instalação, começando com a etapa 5 na página 154.
4. Inicie novamente o serviço do agente.

   Para iniciar novamente o serviço do agente, clique em:

   Iniciar → Configurações → Painel de Controle → Ferramentas Administrativas → Serviços

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 1585
3698
Doc.

O painel Serviços é exibido. Clique com o botão direito do mouse em **Agente ITSANM**. Dê um clique em **Iniciar**.

Instalando o Pacote de Idiomas no AIX

Siga estas etapas para instalar o Pacote de Idiomas no host gerenciado para o AIX:

1. Pare o serviço do agente. Para parar o serviço do agente no AIX, acesse o diretório de trabalho e execute este comando (utilizando o diretório padrão):

   ```
   /tivoli/itsanm/agent/bin/aix/tcstop.sh
   ```

2. Insira o CD do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
3. Execute estes comandos para executar o script de instalação: :

   ```
   mount -v'cdrfs' -r'' /dev/cd0 /cdrom
   cd /cdrom
   ./setup.aix
   ```

4. Siga as orientações nos painéis de instalação, começando com a etapa 5 na página 154.
5. Inicie novamente o serviço do agente. Para iniciar novamente o serviço do agente no AIX, acesse o diretório de trabalho e execute este comando (utilizando o diretório padrão):

   ```
   /tivoli/itsanm/agent/bin/aix/tcstop.sh
   ```

Instalando o Pacote de Idiomas no Solaris

Siga estas etapas para instalar o Pacote de Idiomas no host gerenciado para o Solaris:

1. Pare o serviço do agente. Para parar o serviço do agente, acesse o diretório de trabalho e execute este comando:

   ```
   /tivoli/itsanm/agent/bin/solaris2/tcstop.sh
   ```

2. Insira o CD do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
3. A unidade deve ser montada manualmente. Utilize estes comandos para alterar para o diretório de montagem e executar o script de instalação:

   ```
   cd /cdrom
   ./setup.sol       (para o Solaris)
   ```

4. Siga as orientações nos painéis de instalação, começando com a etapa 5 na página 154.
5. Inicie novamente o serviço do agente. Para iniciar novamente o serviço do agente, acesse o diretório de trabalho e execute este comando:

   ```
   /tivoli/itsanm/agent/bin/solaris2/tcstart.sh
   ```

Instalando o Pacote de Idiomas no Linux

Siga estas etapas para instalar o Pacote de Idiomas no host gerenciado para o Linux:

1. Pare o serviço do agente. Para parar o serviço do agente, acesse o diretório de trabalho e execute este comando:

   ```
   /tivoli/itsanm/agent/bin/linux/tcstop
   ```

2. Insira o CD do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager na unidade de CD–ROM.
3. Execute os comandos a seguir. Os comandos criam o diretório de CD-ROM, montam o diretório de CD-ROM, alternam para o diretório do agente e depois executam o script de instalação.

```
mkdir /cdrom
mount /dev/cd0 /cdrom
   cd /cdrom/agent
./setup.lin
```

4. Siga as orientações nos painéis de instalação, começando com a etapa 5 na página 154.
5. Inicie novamente o serviço do agente. Para iniciar novamente o serviço do agente, acesse o diretório de trabalho e execute este comando:

   ```
   /tivoli/itsanm/agent/bin/linux/tcstart
   ```

Removendo a Instalação do Pacote de Idiomas

Nota: No gerenciador e no console remoto do Windows: A desinstalação do Pacote de Idiomas do IBM Tivoli Storage Area Network Manager não desinstala o Kit de Idiomas do Tivoli NetView.

Para remover a instalação do Pacote de Idiomas, siga estas etapas:

1. Para o gerenciador do Windows, pare o serviço ITSANM–Manager e o Tivoli NetView Service utilizando o painel Serviços do Windows.

   Para o gerenciador do AIX, pare o gerenciador a partir do diretório de trabalho (utilizando o diretório padrão):

   ```
   /tivoli/itsanm/manager/bin/aix/stopSANM.sh
   ```
2. Se você estiver removendo a instalação do Pacote de Idiomas para o console remoto, pare o Serviço do Tivoli NetView e, em seguida, o serviço do Console do ITSANM por meio do painel Serviços do Windows.
3. Se estiver removendo a instalação do Pacote de Idiomas para o host gerenciado, pare o serviço do Agente ITSANM. Para obter informações sobre como parar o Agente ITSANM, consulte "Instalando o Pacote de Idiomas no Host Gerenciado" na página 163.
4. No diretório em que o Pacote de Idiomas foi instalado, execute estes comandos:
   - Para o Windows, utilize Adicionar ou remover programas. Na barra de ferramentas, clique no seguinte:

     ```
     Iniciar -> Configurações -> Painel de Controle
     ```

     No Painel de Controle, dê um clique duplo em **Adicionar ou remover programas**. Localize e realce o componente que deseja remover. Clique em **Remover**.
   - Para o UNIX, execute _uninstall. Se você tiver utilizado o diretório padrão, poderá executar este comando:

     ```
     tivoli/itsanm/LangPacks/_uninstall
     ```
5. O painel Selecione um Idioma é exibido. Selecione um idioma e clique em **OK** para continuar.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1586
Doc. 3698

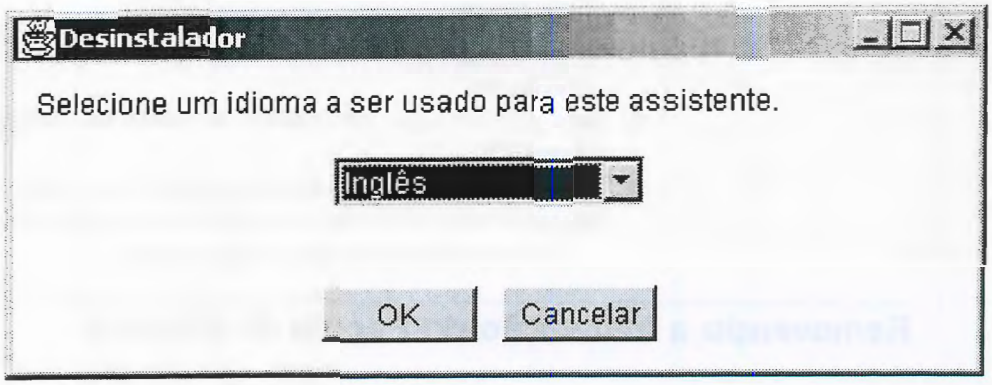


Figura 134. Painel Selecione um Idioma

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

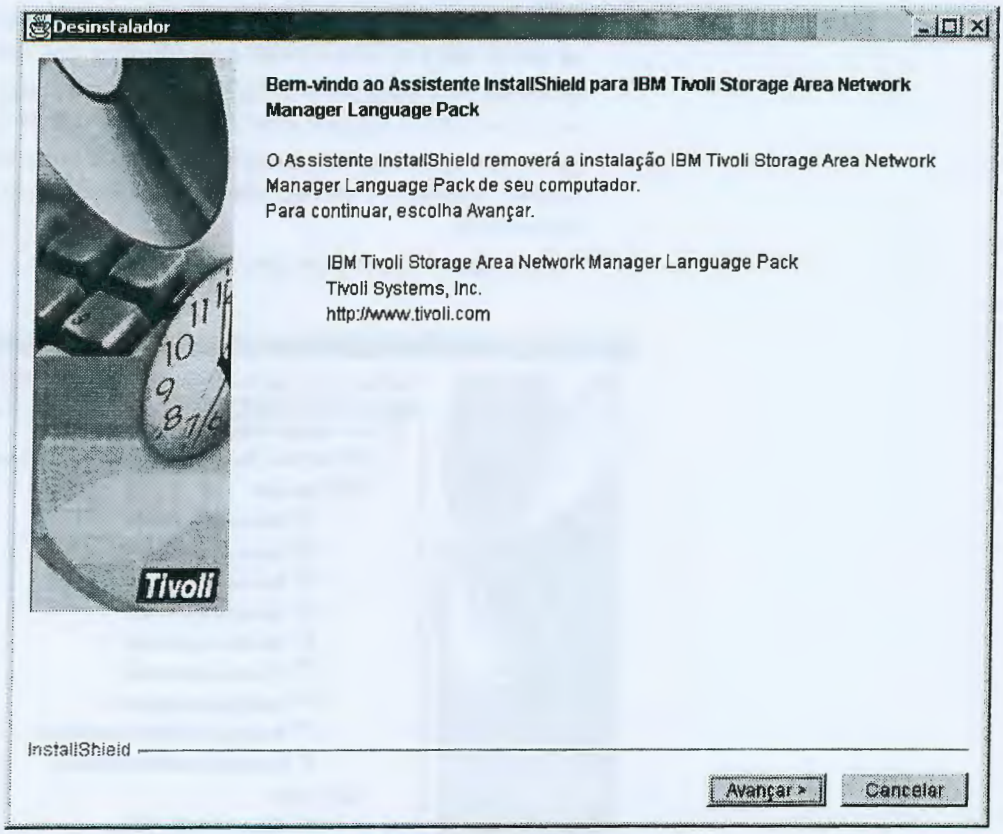


Figura 135. Painel Bem-vindo

7. O painel Selecione os Recursos é exibido. As informações nesse painel são alteradas dependendo do componente do qual você está removendo a instalação e dos idiomas instalados no sistema.

   Se você estiver desinstalando o Pacote de Idiomas para o gerenciador, marque as caixas para o Gerenciador e os idiomas que deseja desinstalar.

   Se estiver desinstalando o Pacote de Idiomas para o host gerenciado, marque as caixas para o Agente e os idiomas que deseja desinstalar.

   Se estiver removendo a instalação do Pacote de Idiomas para o console remoto, marque as caixas para o Console Remoto e os idiomas que deseja desinstalar.

   Clique em **Avançar** para continuar.

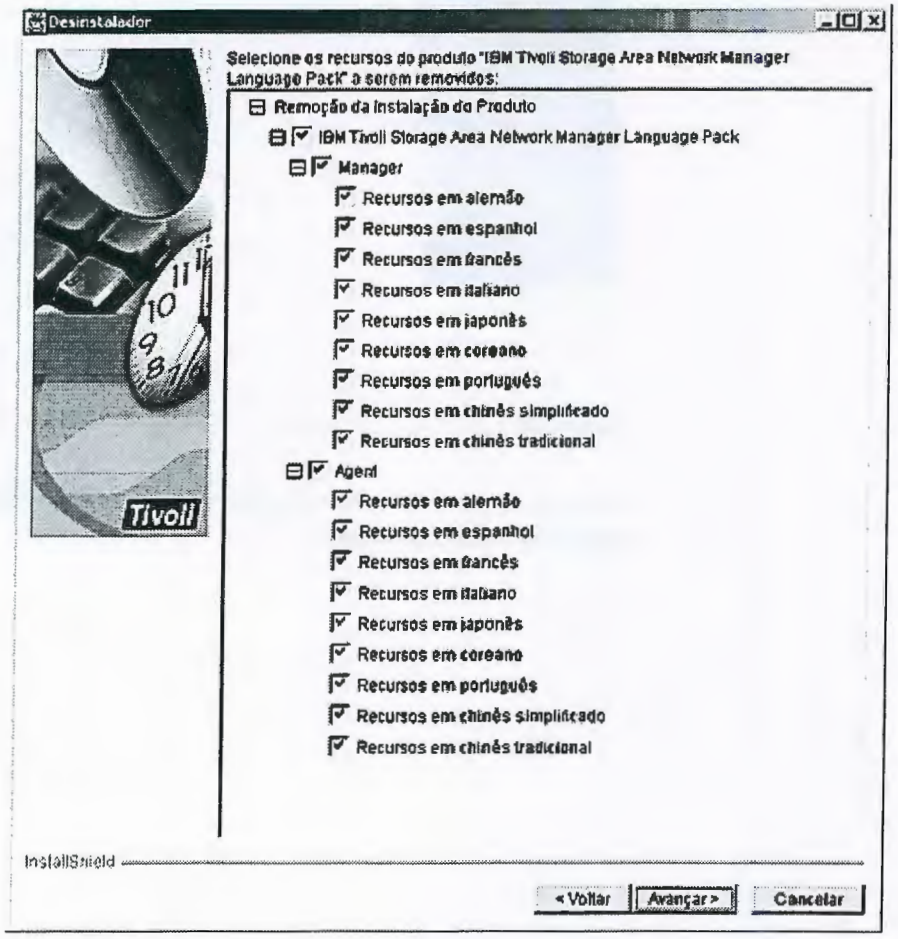


Figura 136. Painel Selecione os Recursos

8. O painel Informações é exibido. Esse painel exibe suas opções de instalação. Revise essas informações e clique em **Avançar** para continuar.

   Nota: Se você estiver desinstalando o Pacote de Idiomas no UNIX, o caminho do diretório será diferente do Windows. Por exemplo, o caminho do diretório do UNIX seria /tivoli/itsanm/LangPacks.

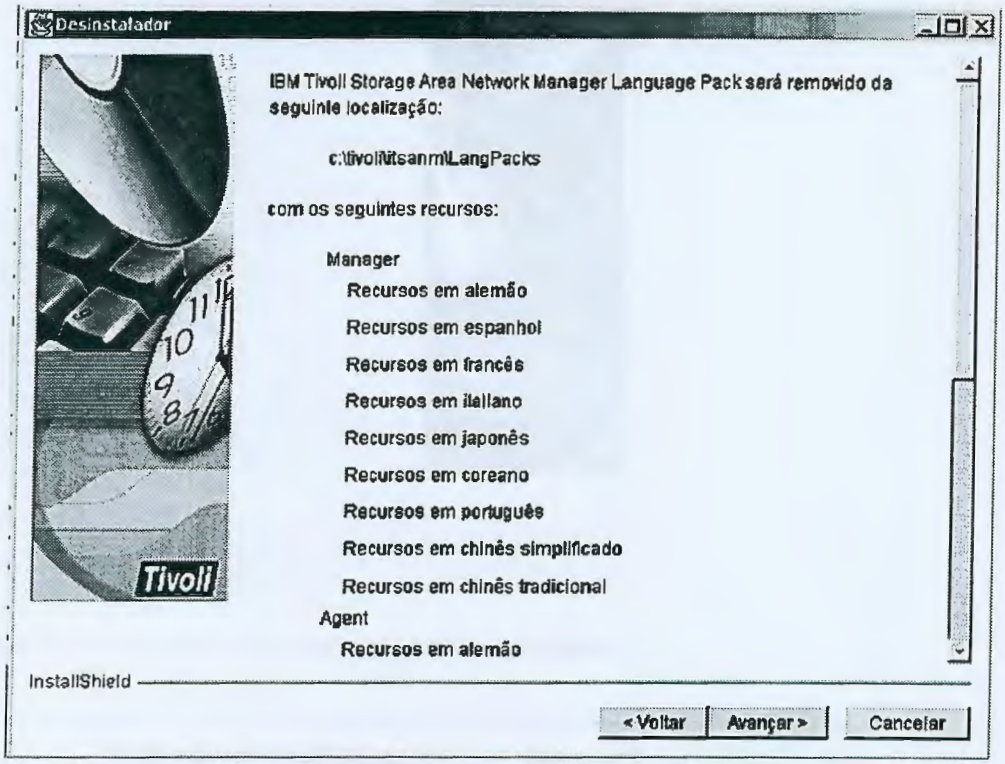


Figura 137. Painel Informações

9. O prompt para a caixa de diálogo Remover Arquivo Existente é exibido. Selecione uma opção:
   - **Sim** para remover o arquivo atual.
   - **Sim para todos** para remover todos os arquivos sem exibir prompts.
   - **Não** para não remover o arquivo atual.
   - **Não para todos** para não remover nenhum arquivo.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1588
Fls. Nº
3698
Doc

10. O painel Instalação Removida com Êxito é exibido. Clique em **Concluir** para concluir a remoção da instalação.

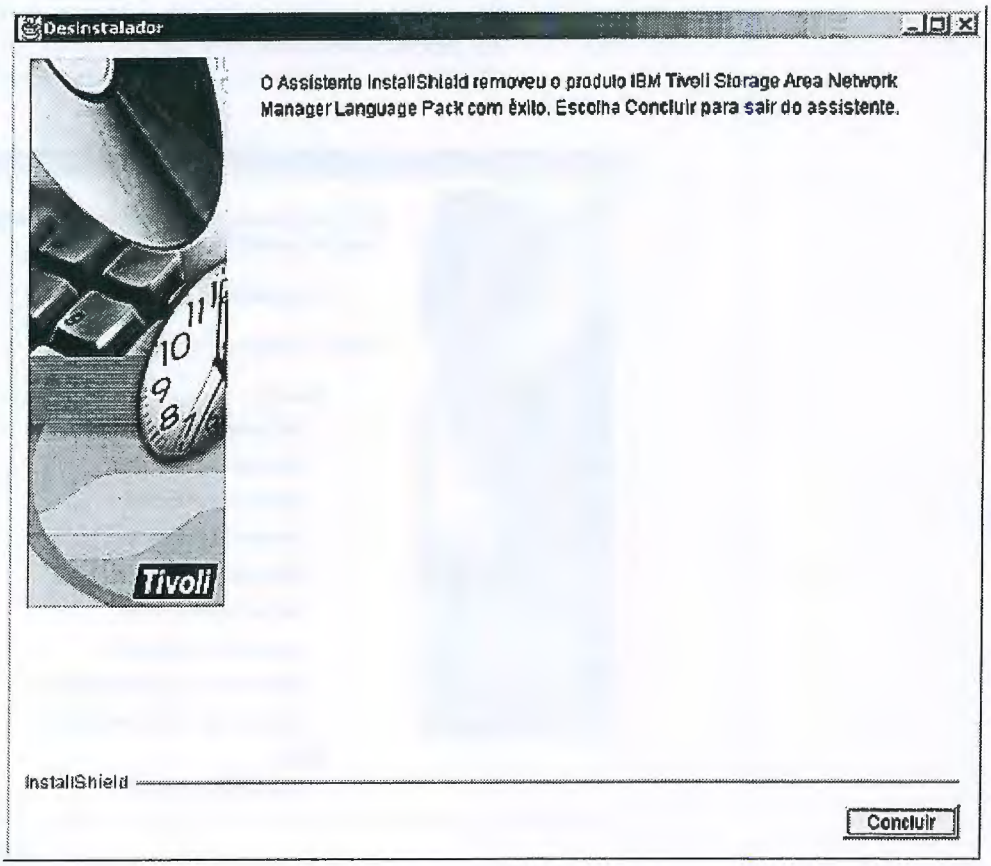


Figura 138. Painel Instalação Removida com Êxito

11. Para o gerenciador do Windows, inicie o Serviço do Tivoli NetView e o serviço ITSANM por meio do painel Serviços do Windows.

    Para o gerenciador do AIX, inicie o gerenciador a partir diretório de trabalho e execute este comando (utilizando o diretório padrão):

    ```
    /tivoli/itsanm/manager/bin/aix/startSANM.sh
    ```

12. Para o console remoto, inicie o Serviço do Tivoli NetView e, em seguida, inicie o Console do ITSANM por meio do painel Serviços do Windows.
13. Para os hosts gerenciados, inicie novamente o agente. Para obter informações sobre como iniciar novamente os agentes, consulte "Instalando o Pacote de Idiomas no Host Gerenciado" na página 163.

Capítulo 12. Removendo a Instalação do IBM Tivoli Storage Area Network Manager

Esta seção descreve como remover a instalação do IBM Tivoli Storage Area Network Manager nas máquinas do gerenciador, console e host gerenciado.

Nota:

- No gerenciador do Windows: Se você instalou o gerenciador e o Tivoli NetView foi instalado com ele, o procedimento de desinstalação também desinstalará o Tivoli NetView. Se tiver instalado o gerenciador e o Tivoli NetView não tiver sido instalado com esse gerenciador (o Tivoli NetView já estava instalado), a instalação do Tivoli NetView não será removida.
- Se tiver instalado o console remoto e o Tivoli NetView tiver sido instalado com esse console remoto, o procedimento de remoção da instalação também removerá a instalação do Tivoli NetView. Se tiver instalado o console remoto e o Tivoli NetView não tiver sido instalado com esse console remoto (o Tivoli NetView já estava instalado), a instalação do Tivoli NetView não será removida.
- Se estiver desinstalando o IBM Tivoli Storage Area Network Manager e o DB2, deverá desinstalar os produtos nesta seqüência:
  1. IBM Tivoli Storage Area Network Manager
  2. DB2

Esta seção fornece informações sobre os seguintes itens:

Item	Consulte
Como Instalar o Gerenciador no Windows	"Desinstalando o Gerenciador no Windows"
Como Instalar o Gerenciador no AIX	"Desinstalando o Gerenciador no AIX" na página 177
Como Desinstalar os Agentes	"Desinstalando os Agentes" na página 182
Como Desinstalar o Console Remoto	"Removendo a Instalação do Console Remoto do IBM Tivoli Storage Area Network Manager" na página 178
Como Desinstalar o DB2	"Removendo a Instalação do DB2" na página 186

Desinstalando o Gerenciador no Windows

Antes de remover a instalação do gerenciador, feche todas as janelas do Tivoli NetView. Quando o IBM Tivoli Storage Area Network Manager é instalado, também instala o pacote GUID Tivoli. A instalação desse pacote GUID não é removida quando você remove a instalação do IBM Tivoli Storage Area Network Manager. Se você planeja reinstalar o IBM Tivoli Storage Area Network Manager, não deve excluir os arquivos e diretórios específicos do GUID Tivoli. Isso pode fazer com que o IBM Tivoli Storage Area Network Manager funcione incorretamente. Os arquivos e diretórios específicos do GUID Tivoli são os seguintes:

© Copyright IBM Corp. 2002, 2003

CPMI CORREIOS
Fls. Nº 1589
Doc. 3698

Tabela 15. Diretórios do GUID Tivoli

Plataforma	Diretório
AIX	/usr/tivoli/guid
Solaris	/opt/tivoli/guid
Windows	Arquivos de programas\tivoli\guid

Normalmente, você não removeria a instalação do pacote GUID Tivoli. Entretanto, se quiser limpar o computador, poderá remover a instalação desse pacote manualmente. Para obter informações sobre como remover a instalação do GUID Tivoli, consulte "Removendo a Instalação do Pacote GUID Tivoli" na página 177.

Para remover a instalação do gerenciador, siga estas etapas:

1. Na barra de ferramentas, clique no seguinte:
   `Iniciar → Configurações → Painel de Controle`
2. No Painel de Controle, dê um clique duplo em **Adicionar ou remover programas**.
3. Dê um clique com o botão direito do mouse em IBM WebSphere Application Server V5 – ITSANM–Manager.
4. Clique em **Remover**.
5. O painel Selecione um Idioma é exibido. Selecione **Português (Brasil)** e clique em **OK**.

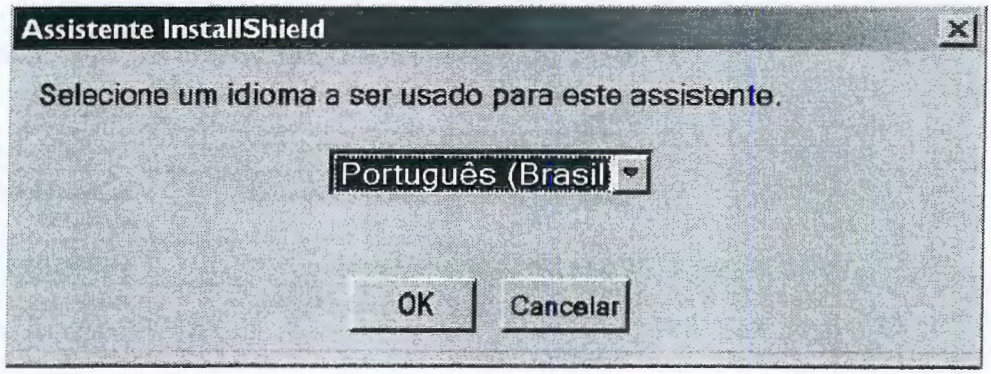


Figura 139. Painel Selecione um Idioma

10126
A.

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

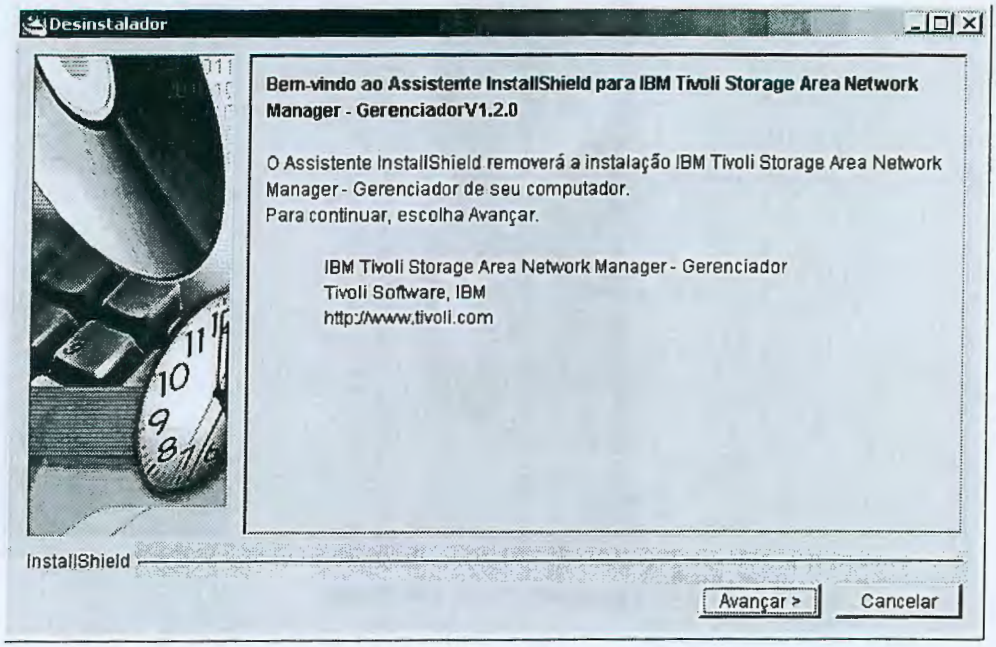


Figura 140. Painel Bem-vindo

7. O painel Localização é exibido. Ele fornece informações sobre a localização da qual a instalação do gerenciador será removida. Clique em **Avançar** para continuar.

   Nota: O nome do caminho UNIX no painel é diferente do utilizado no Windows. Por exemplo, no UNIX, o nome do caminho seria /tivoli/itsanm/manager.

ROS nº 03/2004 - SIN
CPMI - CORREIOS
Fls. Nº 1590
Doc 3698

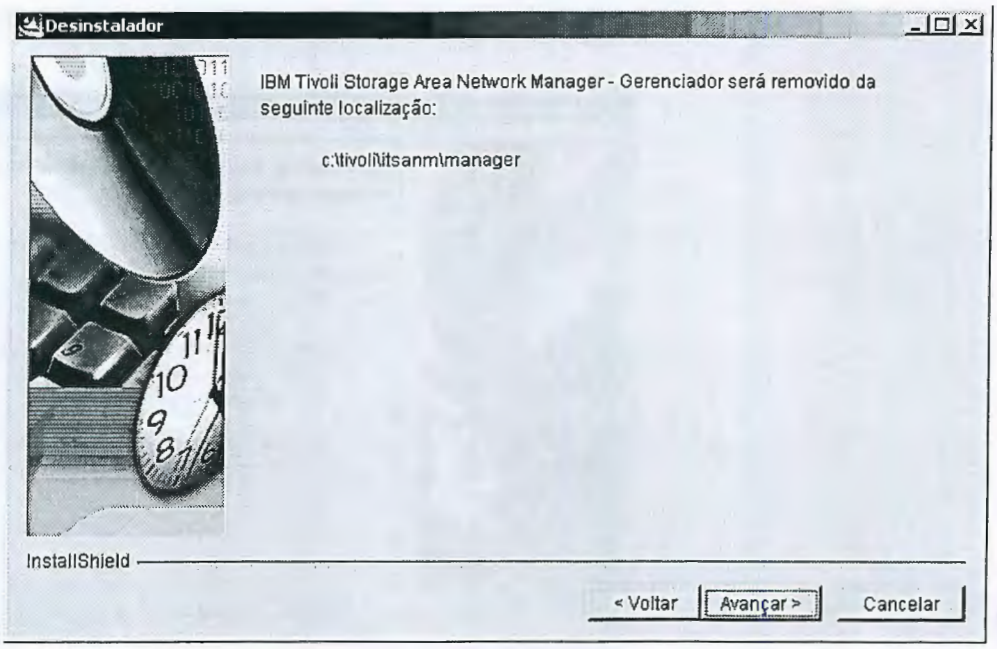


Figura 141. Painel Localização

8. O painel Removendo a Instalação é exibido. Essa etapa pode demorar algum tempo para remover a instalação.

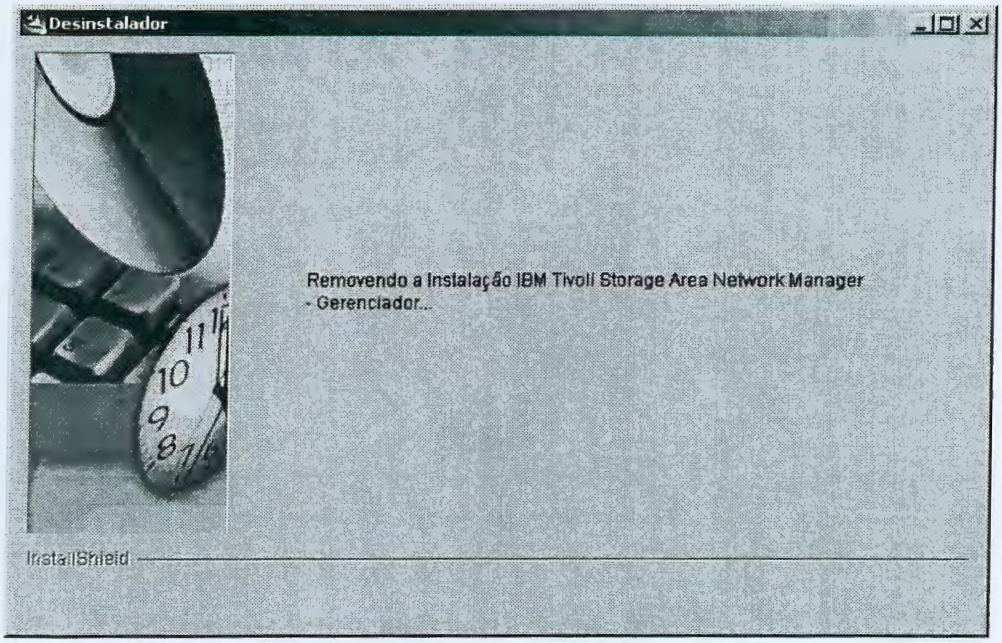


Figura 142. Painel Removendo a Instalação

9. O prompt para a caixa de diálogo Remover Arquivo Existente é exibido.
   - **Sim** para remover o arquivo atual.
   - **Sim para todos** para remover todos os arquivos sem exibir prompts.
   - **Não** para não remover o arquivo atual.
   - **Não para todos** para não remover nenhum arquivo.

   Selecione uma opção.

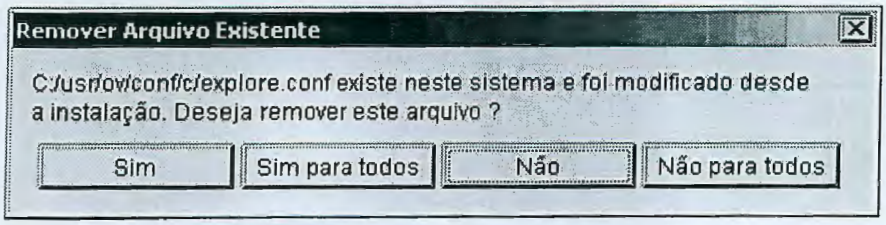


Figura 143. Caixa de Diálogo Remover Arquivo Existente

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1591
Doc. 3698

10. O painel Instalação Removida com Êxito é exibido. Clique em **Avançar**.

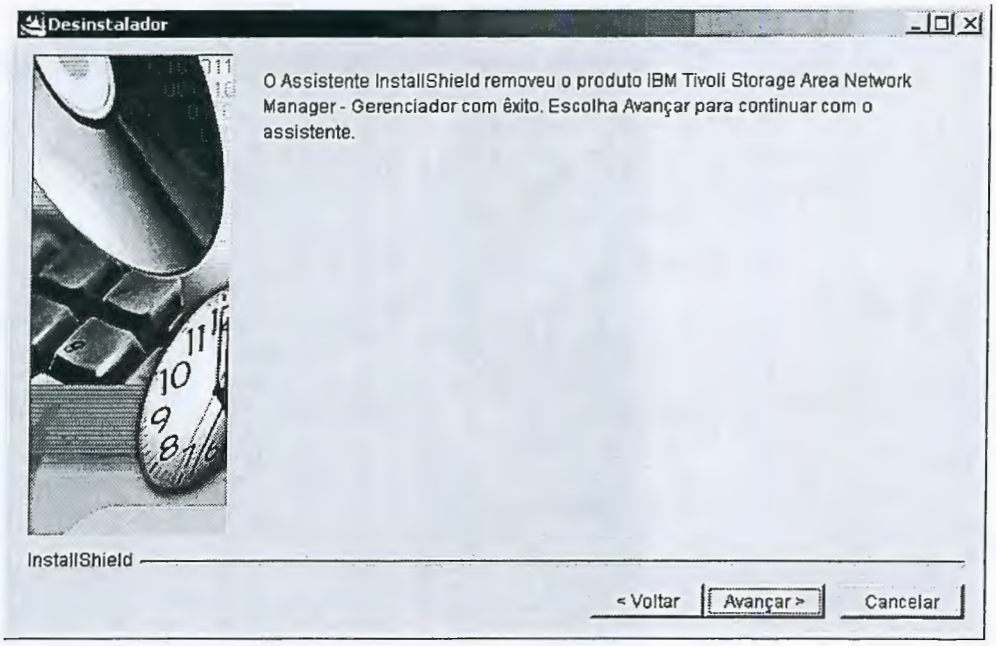


Figura 144. Painel Instalação Removida com Êxito

11. O painel Inicie Novamente o Sistema é exibido. É possível selecionar **Sim** para iniciar novamente o sistema agora ou **Não** para iniciá-lo novamente mais tarde. O sistema deve ser reinicializado após a remoção da instalação do gerenciador para que essa remoção seja concluída com êxito.

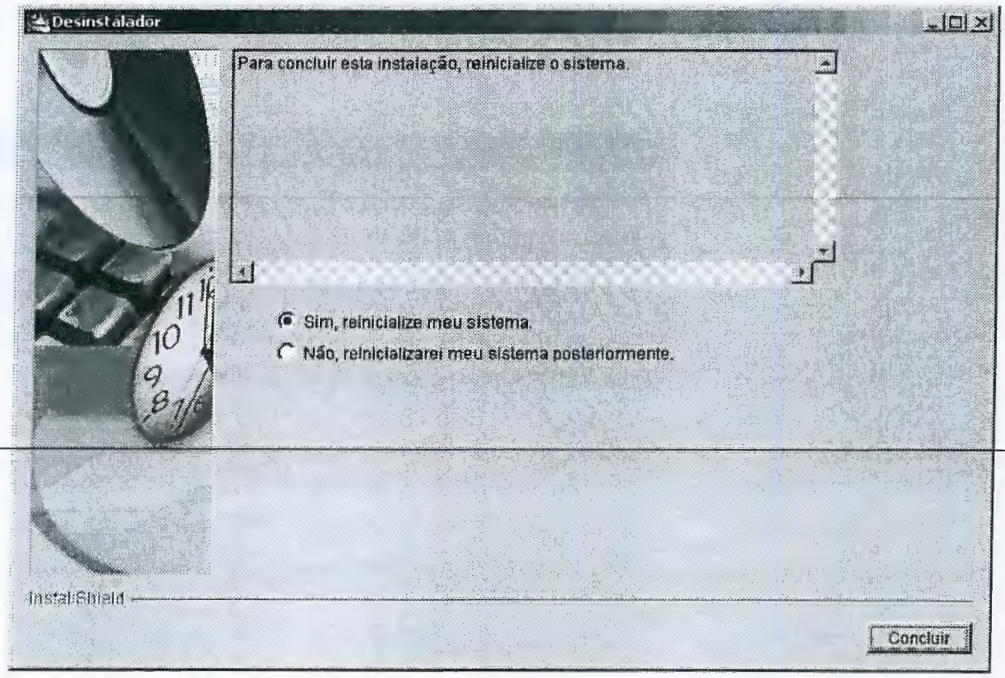


Figura 145. Painel Inicie Novamente o Sistema

Removendo a Instalação do Pacote GUID Tivoli

O pacote GUID Tivoli é utilizado para resolver a identificação de um computador. Computadores podem ter vários nomes de domínio, um endereço IP dinâmico que é alterado ou um nome de host que é alterado. O pacote GUID permite que o computador tenha um identificador exclusivo global. Isso garante que um computador que esteja executando vários aplicativos possa ser exclusivamente identificado. Por exemplo, um computador pode estar executando o cliente Tivoli Storage Manager e o agente do IBM Tivoli Storage Area Network Manager.

Nota: Normalmente, você não removeria a instalação do pacote GUID Tivoli. As informações a seguir são fornecidas caso você queira ter um computador limpo. Se você tiver outros aplicativos Tivoli utilizando o pacote GUID, não remova a instalação desse pacote.

Para remover a instalação do pacote GUID Tivoli no AIX, insira este comando:

```
installp -u tivoli.tivguid
```

Também é possível remover a instalação do pacote GUID Tivoli utilizando **smitty**.

Para remover a instalação do pacote GUID Tivoli no Solaris, insira este comando:

```
pkgrm TIVguid
```

Para remover a instalação do pacote GUID Tivoli no Windows, siga estas etapas:

1. Acesse a barra de ferramentas e clique em:

   `Iniciar -> Configurações -> Painel de Controle`
2. No Painel de Controle, dê um clique duplo em **Adicionar ou remover programas**.
3. A caixa de diálogo Adicionar ou remover programas é exibida. Na guia Instalar/Desinstalar, selecione**TivGUID**.
4. Clique em **Remover**.

Desinstalando o Gerenciador no AIX

Quando o IBM Tivoli Storage Area Network Manager é instalado, também instala o pacote GUID Tivoli. A instalação desse pacote GUID não é removida quando você remove a instalação do IBM Tivoli Storage Area Network Manager. Se você planeja reinstalar o IBM Tivoli Storage Area Network Manager, não deve excluir os arquivos e diretórios específicos do GUID Tivoli. Isso pode fazer com que o IBM Tivoli Storage Area Network Manager funcione incorretamente.

Para remover a instalação do gerenciador, siga estas etapas:

1. O programa de remoção da instalação é criado no diretório de instalação após a instalação do agente. Execute **uninstall** no diretório **installdir/manager/_uninst** para desinstalar o gerenciador. No diretório **raiz**, insira este comando:

   `/tivoli/itsanm/manager/_uninst/uninstall`
2. Siga as etapas da desinstalação do Windows a partir da etapa 5 na página 172 (o painel Selecione um Idioma).
3. Não é necessário reinicializar o sistema. Porém, para reutilizar as portas do gerenciador (9550–9556), você deverá reinicializar o sistema.

10122 A
CPMI - CORREIOS
Fls Nº 1592
Nº Doc 3698

Removendo a Instalação do Console Remoto do IBM Tivoli Storage Area Network Manager

Antes de remover a instalação do console remoto, feche todas as janelas do Tivoli NetView.

Para remover a instalação do Console remoto do IBM Tivoli Storage Area Network Manager, siga estas etapas:

1. Na barra de ferramentas, clique no seguinte:

   `Iniciar → Configurações → Painel de Controle`
2. No Painel de Controle, dê um clique duplo em **Adicionar ou remover programas**.
3. Localize e realce ITSANM – Console.
4. Clique em **Remover**.
5. O painel Selecione um Idioma é exibido. Selecione um idioma. Clique em **OK**.

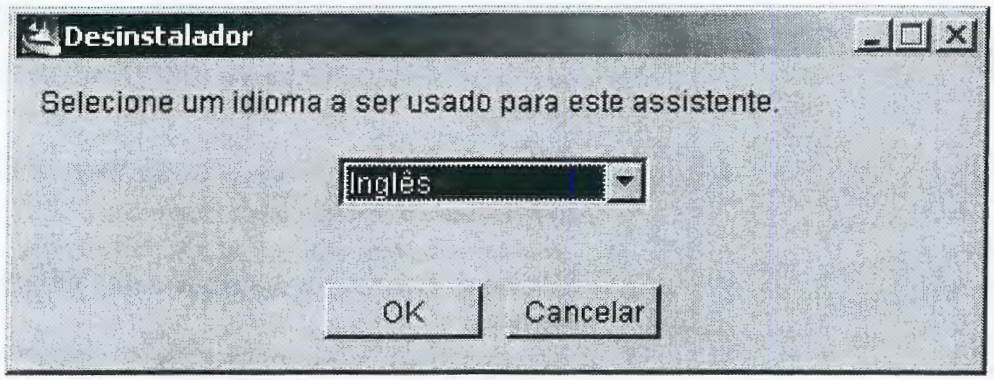


Figura 146. Painel Selecione um Idioma

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

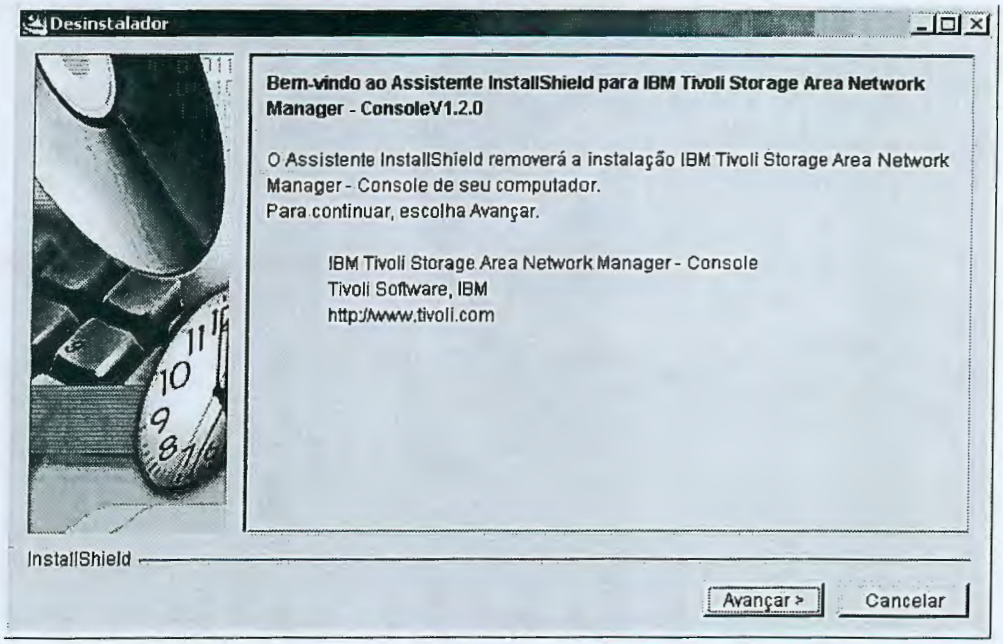


Figura 147. Painel Bem-vindo

7. O painel Localização é exibido. Clique em **Avançar** para continuar.

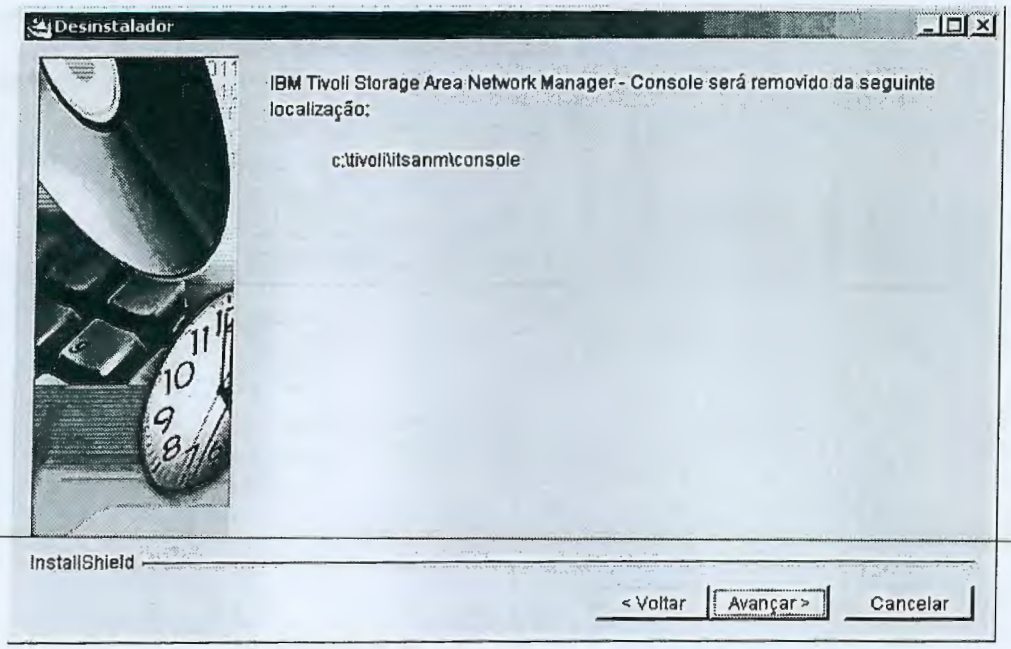


Figura 148. Painel Localização

8. O painel Removendo a Instalação é exibido.

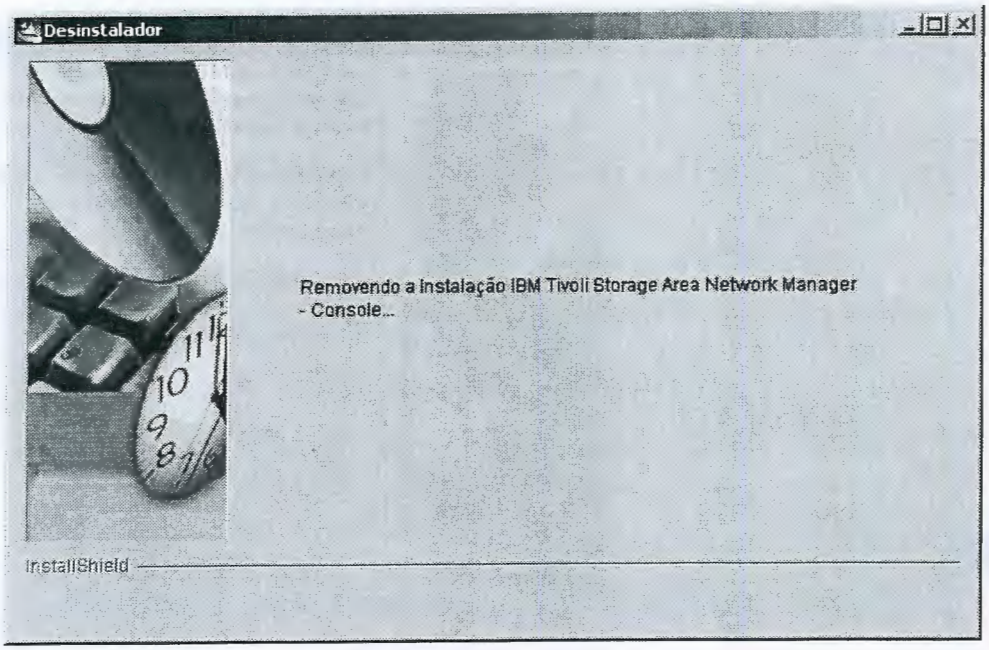


Figura 149. Painel Removendo a Instalação

9. O prompt para a caixa de diálogo Remover Arquivo Existente é exibido. Selecione uma opção:
   - **Sim** para remover o arquivo atual.
   - **Sim para todos** para remover todos os arquivos sem exibir prompts.
   - **Não** para não remover o arquivo atual.
   - **Não para todos** para não remover nenhum arquivo.

10. O painel Instalação Removida com Êxito é exibido. Clique em **Avançar**.

Figura 150. Painel Instalação Removida com Êxito

11. O painel Inicie Novamente o Sistema é exibido. É possível selecionar **Sim** para iniciar novamente o sistema agora ou **Não** para iniciá-lo novamente mais tarde. O sistema deve ser reinicializado após a remoção da instalação do console remoto para que essa remoção seja concluída com êxito. Clique em **Concluir**.

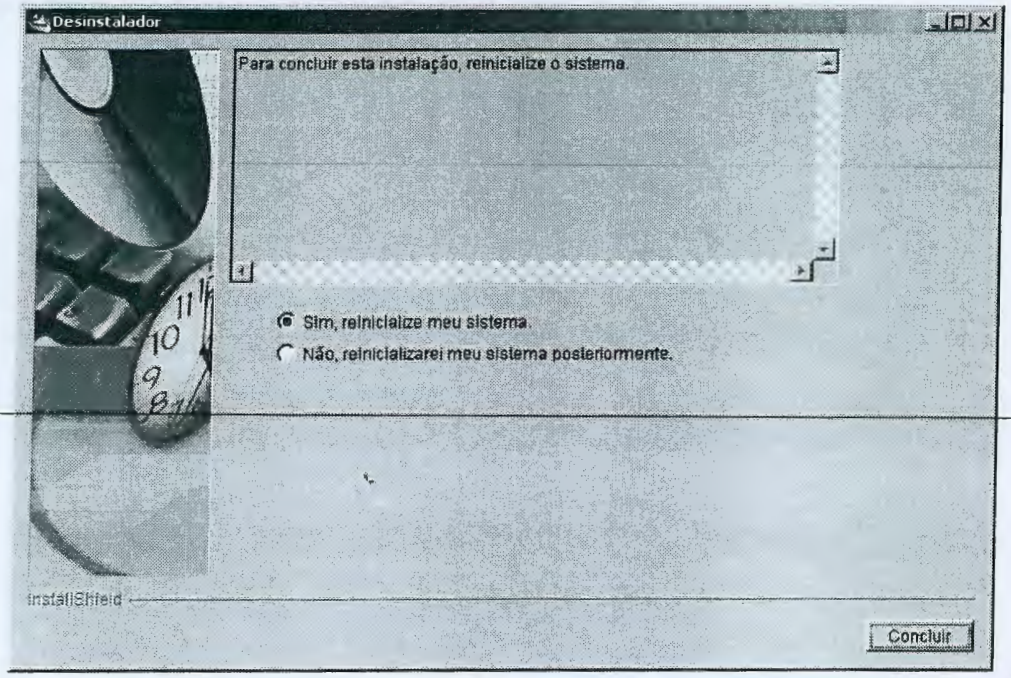


Figura 151. Painel Inicie Novamente o Sistema

CPMI CORREIOS
Fls. Nº 1594
Doc. 3698

Desinstalando os Agentes

Esta seção descreve como desinstalar os agentes em plataformas diferentes.

Desinstalando o Agente no Windows

Para remover a instalação do agente no Windows, siga estas etapas:

1. Verifique se o serviço do agente está parado.
2. No diretório de remoção da instalação, dê um clique duplo em **Adicionar ou remover programas**.
3. Localize e realce ITSANM – Agent.
4. Clique em **Remover**.
5. O painel Selecione um Idioma é exibido. Selecione um idioma. Clique em **OK**.

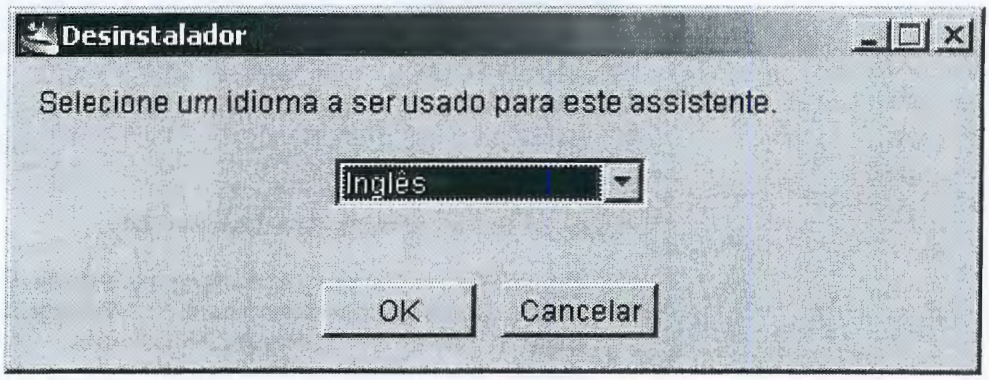


Figura 152. Painel Selecione um Idioma

6. O painel Bem-vindo é exibido. Clique em **Avançar** para continuar.

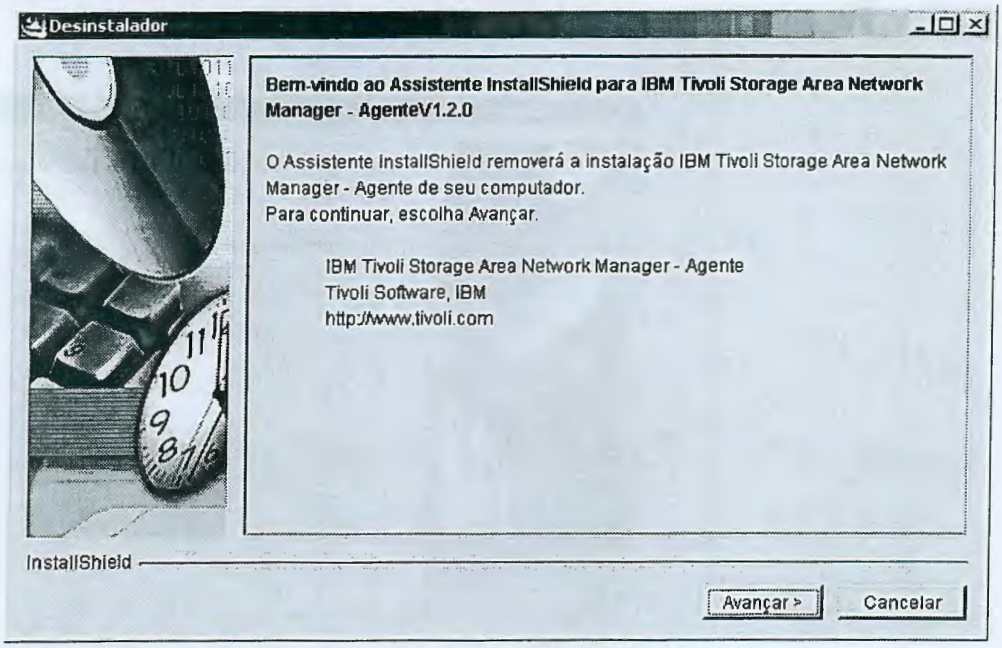


Figura 153. Painel Bem-vindo

7. O painel Remover Instalação do Diretório é exibido. Clique em **Avançar** para continuar.

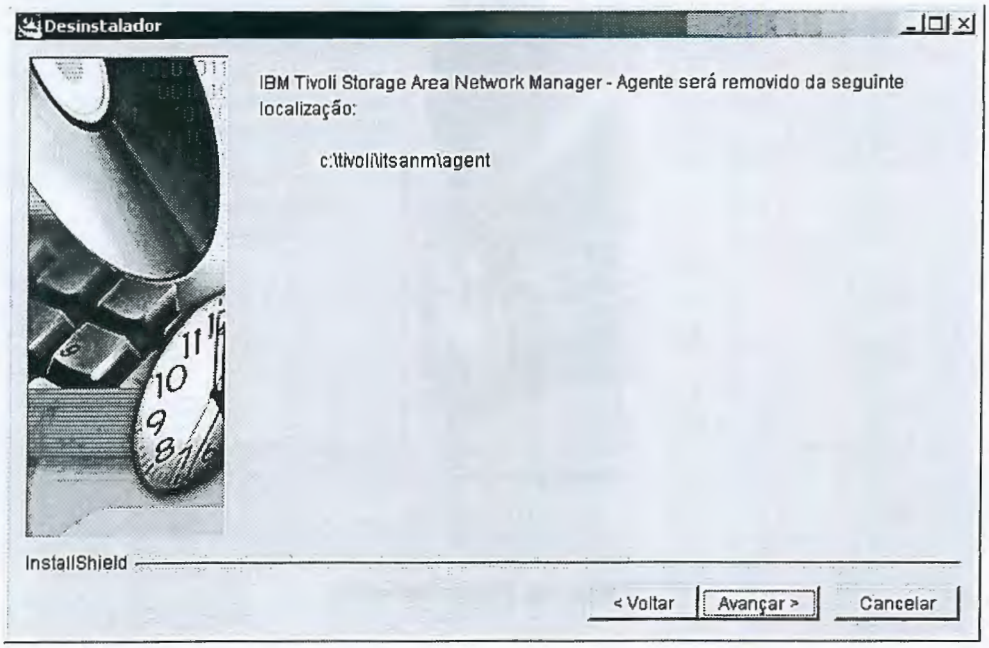


Figura 154. Painel Remover Instalação do Diretório

8. O prompt para a caixa de diálogo Remover Arquivo Existente é exibido. Selecione uma opção:
   - **Sim** para remover o arquivo atual.
   - **Sim para todos** para remover todos os arquivos sem exibir prompts.
   - **Não** para não remover o arquivo atual.
   - **Não para todos** para não remover nenhum arquivo.
9. O painel Removendo a Instalação é exibido.

10. O painel Instalação Removida com Êxito é exibido. Clique em **Avançar**.

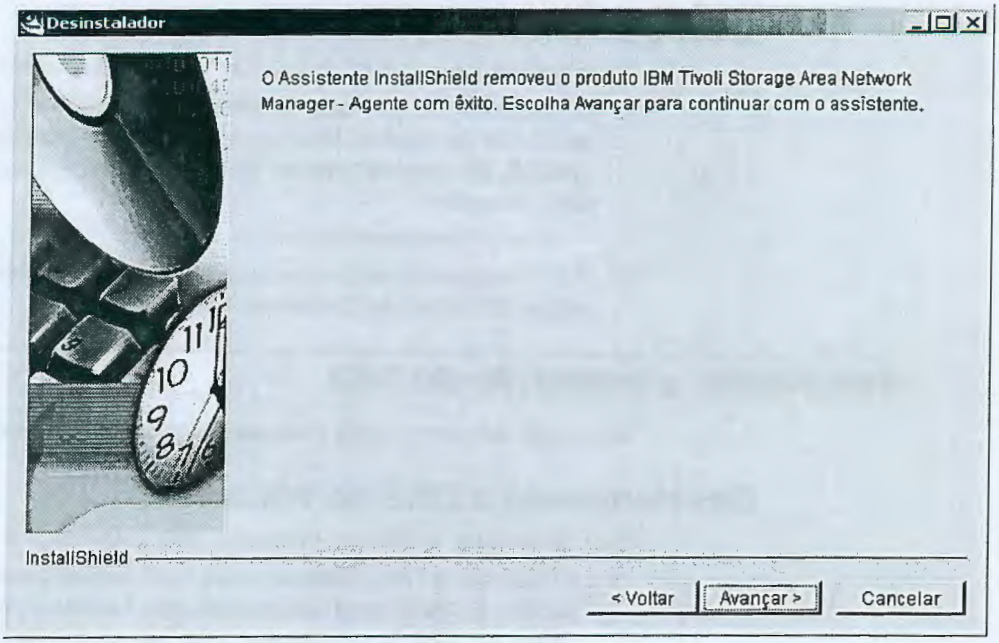


Figura 155. Painel Instalação Removida com Êxito

Desinstalando o Agente no AIX ou Solaris

Para remover a instalação do agente no AIX ou Solaris, siga estas etapas:

1. Verifique se o serviço do agente está parado.Execute este comando:

```
ps -aef | grep "java.*tsnm.baseDir"
```

Se você *não* visualizar esta entrada, significa que o serviço do agente foi parado:

```
 root  96498 158924   0   Aug 17  pts/3 24:53 /tivoli/itsanm/
   agent/jre/bin/java
 -Dtsnm.baseDir=/tivoli/itsanm/agent -Dtsnm.localPort=9570
-Dtsnm.protocol=http:
// -Djlog.noLogCmd=true -classpath /tivoli/itsanm/agent/lib/
   classes:/tivoli/itsanm
/agent/servlet/common/lib/servlet.jar:/tivoli/itsanm/agent/lib/
   com.ibm.mq.jar:/ti
voli/itsanm/agent/lib/com.ibm.mqjms.jar:/tivoli/itsanm/agent/lib/
   jms.jar:/tivoli/
itsanm/agent/lib/ServiceManager.jar::/tivoli/itsanm/agent/servlet/
   bin/bootstrap.jar
 -Djavax.net.ssl.keyStore=/tivoli/itsanm/agent/conf/server.keystore
   -Djavax.net.s
sl.keyStorePassword=YourServerKeystorePassword -Dcatalina.
   base=/tivoli/itsanm/age
nt/servlet -Dcatalina.home=/tivoli/itsanm/agent/servlet
   org.apache.catalina.start
   up.Bootstrap start
    root 471386 448550   1 14:35:03  pts/4  0:00
        grep java.*tsnm.baseDir
```

2. O programa de remoção da instalação é criado no diretório de instalação após a instalação do agente. Execute **uninstall** no diretório **installdir/agent/_uninst** para remover a instalação do agente. No diretório **raiz**, insira este comando:

```
/tivoli/itsanm/agent/_uninst/uninstall
```


ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1596
3698
Doc.

3. Siga as etapas da remoção da instalação do Windows começando na etapa 5 na página 182 (o painel Selecione um Idioma).

Desinstalando o Agente com Linux

Para desinstalar o agente com o Linux, siga estas etapas:

1. O programa de remoção da instalação é criado no diretório de instalação após a instalação do agente. Execute **uninstall** sob o diretório **<install_dir>/agent/_uninst** para desinstalar o agente. No diretório **raiz**, insira este comando:

   ```
   /tivoli/itsanm/agent/_uninst/uninstall
   ```

2. Siga as etapas da remoção da instalação do Windows começando na etapa 5 na página 182 (o painel Selecione um Idioma).

Removendo a Instalação do DB2

Esta seção descreve como desinstalar o DB2 no Windows e no AIX.

Desinstalando o DB2 no Windows

Para desinstalar o DB2 no Windows, siga estas etapas:

1. Utilizando o DB2, elimine o banco de dados itsanmdb. Itsanmdb é o nome padrão. Se você tiver renomeado esse banco de dados, elimine o banco de dados do IBM Tivoli Storage Area Network Manager. Para obter informações sobre como eliminar um banco de dados, consulte"Eliminando um Banco de Dados DB2" na página 204.
2. Acesse a barra de ferramentas e clique em:

   ```
   Iniciar → Configurações → Painel de Controle
   ```

3. No Painel de Controle, dê um clique duplo em **Adicionar ou remover programas.**
4. A caixa de diálogo Adicionar ou remover programas é exibida. Na guia Instalar/Desinstalar, selecione**IBM DB2.**
5. Clique em **Adicionar/Remover.**
6. A caixa de diálogo Confirm DB2 deletion é exibida. Clique em **Yes.**

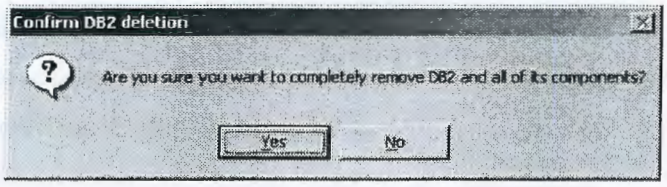


Figura 156. Caixa de diálogo Confirm DB2 deletion

7. O painel Information é exibido. Clique em **Yes.**

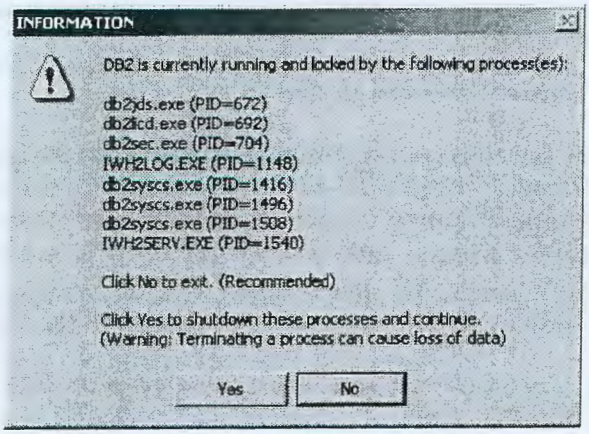


Figura 157. Painel Information

8. A caixa de diálogo Uninstall é exibida. Quando a remoção da instalação estiver concluída, clique em **OK**.

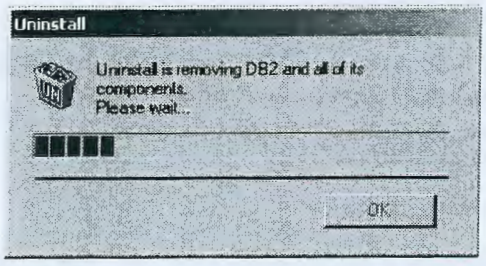


Figura 158. Caixa de Diálogo Uninstall

9. A caixa de diálogo Uninstall com êxito é exibida. Clique em **OK**.

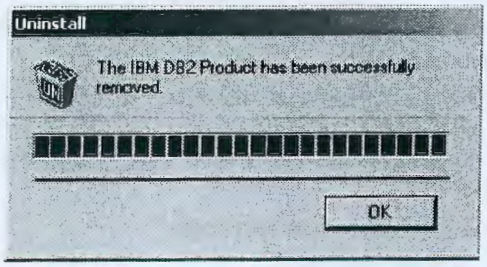


Figura 159. Caixa de Diálogo Uninstall com êxito

10. Certifique-se de ter excluído todas as pastas do DB2 relacionadas.

Desinstalando o DB2 no AIX

Para desinstalar o DB2, siga as próximas etapas. O DB2 Administration Server é tido como db2as. Você deve ter autoridade root para desinstalar o DB2.

1. Elimine todos os bancos de dados do DB2. Cada Instância do DB2 pode ter um ou mais bancos de dados. Vá para cada Instância do DB2 e elimine todos os bancos de dados de cada instância. Efetue log in como proprietário da instância. Execute estes comandos:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1597
Nº 3698
Doc.

```
su - <Nome_do_Proprietário_da_Instância> (efetue login como proprietário
da instância)
   db2 list application (lista todos os bancos de dados)
   db2 drop db <Nome_do_BD>
```

Em que *Nome_do_Proprietário_da_Instância* é a Instância do DB2 (por exemplo, db2inst1). *Nome_do_BD* é o nome do banco de dados que será eliminado. Depois de eliminar o banco de dados você verá esta mensagem:

```
DB20000I O comando DROP DATABASE foi concluído com êxito.
```

2. Pare o servidor de administração. O ID do usuário padrão é **db2as**. Para parar o servidor de administração, execute estes comandos:

```
su - db2as (efetue login como administrador do DB2)
   db2admin stop
```

Depois de parar o servidor de administração você verá esta mensagem:

```
SQL4407W O DB2 Administration Server foi parado com êxito.
```

3. Pare todas as Instâncias do DB2. Para obter uma lista de Instância do DB2, execute este comando:

```
   <DB2_DIR>/bin/db2list
```

DB2_DIR é o diretório do DB2. O padrão é /usr/lpp/db2_07_01. Para cada instância na lista, execute os seguintes comandos:

```
   su - <Nome_do_Proprietário_da_Instância>
   db2 force application all
   db2stop
   db2 terminate
```

Nome_da_Instância é uma Instância do DB2, por exemplo, db2inst1.

4. Remova o servidor de administração. Execute este comando no diretório raiz:

```
/usr/lpp/<programa_DB2>/instance/dasidrop db2as
```

programa_DB2 é o programa do DB2, por exemplo db2_07_01.

5. Remova todas as Instâncias do DB2. Para cada Instância do DB2, execute o seguinte comando:

```
   <DB2_DIR>/instance/db2idrop <Nome_da_Instância>
```

DB2_DIR é o diretório do DB2 e *Nome_da_Instância* o nome da instância, por exemplo, db2inst1.

6. Remova o DB2. Execute este comando:

```
   installp -u <programa_DB2>
```

Em que *programa_DB2* é o nome do programa DB2, por exemplo, db2_07_01.

7. Remova o nome da instância na lista de usuários (opcional, porém recomendado). Execute **smit** e vá para estes painéis:

```
   Segurança & Usuários
Usuários   Remover um usuário
   Remover um Usuário do Sistema
```

Remova o nome da instância (por exemplo, db2inst1) e o nome do Servidor de Administração (por exemplo, db2as).

8. Reinicialize a máquina (opcional, porém recomendado).

10110
A.

Apêndice A. Instalação Silenciosa do IBM Tivoli Storage Area Network Manager

Antes de instalar o gerenciador, certifique-se de que fez o trabalho de planejamento da pré-instalação, conforme descrito no Capítulo 3, "Preparando-se para a Instalação (Gerenciador do Windows)", na página 19 para Windows ou no Capítulo 4, "Preparando-se para a Instalação (Gerenciador do AIX)", na página 35 para AIX.

O IBM Tivoli Storage Area Network Manager suporta instalações silenciosas e não-assistidas. Modificando os parâmetros apropriados no arquivo de opções do gerenciador, console remoto ou agente, você poderá então executar o script para instalar o componente. Se você instalar o IBM Tivoli Storage Area Network Manager utilizando a instalação silenciosa, deverá desinstalar o produto utilizando o mesmo procedimento.

Instalando o Gerenciador

O arquivo de opções do gerenciador localiza-se no diretório de instalação do gerenciador. O arquivo de opções chama-se **manager.opt**. Para poder instalar o gerenciador, você deve alterar os parâmetros apropriados no arquivo de opções. Consulte Figura 160.

```
###############################################################################
# InstallShield Options File Template for Manager silent install
#
# This file can be used to create an options file (i.e., response file) for the
# wizard "Setup". Options files are used with "-options" on the command line to
# modify wizard settings.
#
# The settings that can be specified for the wizard are listed below. To use
# this template, follow these steps:
#
#    1. Specify a value for a setting by replacing the characters 'value'.
#    Read each settings documentation for information on how to specify its
#    value.
#
#    2. Save the changes to the file.
#
#    3. To use the otpions file with the wizard, specify -options filename
#    as a command line argument to the wizard, where filename is the name
#    of this options file.
#    example:
#      setup.exe -silent -options manager.opt
#
#
###############################################################################

#------------------------------------------------------------------------------
# Selecione o idioma padrão
# Exemplo:
#  -P defaultLocale="English"
#------------------------------------------------------------------------------
#-P defaultLocale="English"
```

Figura 160. Arquivo Manager.opt (Parte 1 de 3)

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1598
3698
Doc.

```
#-------------------------------------------------------------------------------
# Installation destination directory. Specify a valid directory into which the
# product should be installed. If the directory contains spaces, enclose it in
# double-quotes. For example, to install the product to C:\Program Files\My
# Product in Windows, use
# -P installLocation="C:\Program Files\My Product"
#  -P installLocation="C:/tivoli/itsanm/manager"
# For Unix
#  -P installLocation="/tivoli/itsanm/manager"
#-------------------------------------------------------------------------------
-P installLocation="C:/tivoli/itsanm/manager"
#-------------------------------------------------------------------------------
# Base port number for this installation
# Example:
#  -W portNoBean.portNumber=9550
#-------------------------------------------------------------------------------
-W portNoBean.portNumber=9550

#-------------------------------------------------------------------------------
# DB2 administrator user ID
# Example:
#  -W DBPassword.userID="db2admin"
#-------------------------------------------------------------------------------
-W DBPassword.userID="db2admin"

#-------------------------------------------------------------------------------
# DB2 administrator password
#
# Example:
#  -W DBPassword.password="password"
#-------------------------------------------------------------------------------
-W DBPassword.password="password"

#-------------------------------------------------------------------------------
# Name of database to be created and used by SANM (SANM database)
#
# Exemplo:
#  -W SANPassword1.dbName="itsanmdb"
#-------------------------------------------------------------------------------
-W SANPassword1.dbName="itsanmdb"

#-------------------------------------------------------------------------------
# SANM database user ID, must be different than DB2 administrator user ID
#
# Example:
#  -W SANPassword1.userID="db2user1"
#-------------------------------------------------------------------------------
-W SANPassword1.userID="db2user1"

#-------------------------------------------------------------------------------
# SANM database password
# Example:
#  -W SANPassword1.userID="password"
#-------------------------------------------------------------------------------
-W SANPassword1.password="password"
```

Figura 160. Arquivo Manager.opt (Parte 2 de 3)

```
#-------------------------------------------------------------------------------
# Websphere user ID
# Example:
#  -W WASPassword.userID="wasuser1"
#-------------------------------------------------------------------------------
-W WASPassword.userID="db2user1"

#-------------------------------------------------------------------------------
# Websphere password for the user above
# Example:
#  -W WASPassword.password="password"
#-------------------------------------------------------------------------------
-W WASPassword.password="password"

#-------------------------------------------------------------------------------
# Manager, Agent, Console communication password
# Example:
#  -W comPassword.password="password"
#-------------------------------------------------------------------------------
-W comPassword.password="password"

#-------------------------------------------------------------------------------
# Drive Letter where Netview to be installed.
# Exemplo:
#  -W beanNVDriveInput.chcDriveName="C"
#-------------------------------------------------------------------------------
-W beanNVDriveInput.chcDriveName="C"

#-------------------------------------------------------------------------------
# Netview password.
# Example:
#  -W beanNetViewPasswordPanel.password="password"
#-------------------------------------------------------------------------------
-W beanNetViewPasswordPanel.password="password"

#-------------------------------------------------------------------------------
# Property use by installation program.  Do not remove or modify.
#-------------------------------------------------------------------------------
-W setWinDestinationBean.value="$P(installLocation)"
```

Figura 160. Arquivo Manager.opt (Parte 3 de 3)

Altere apenas os parâmetros listados a seguir. Não altere nenhum outro parâmetro.

- Especifique o diretório de destino de instalação. No Windows, para que o diretório de destino da instalação seja `C:/myhost/itsanm/manager`, insira o exemplo da seguinte forma:

  ```
  -P installLocation="C:/myhost/itsanm/manager"
  ```

  No gerenciador do AIX, insira o exemplo da seguinte forma:

  ```
  -P installLocation="/myhost/itsanm/manager"
  ```

  Nota: Este procedimento aceita as barras normal e invertida para caminhos de diretórios em uma plataforma Windows.

- Especifique o número da porta base. Por exemplo, você deseja que esse número seja 9800.

  ```
  -W portNoBean.portNumber=9800
  ```

- Especifique o ID do usuário administrador do DB2. Por exemplo, você deseja que o ID do usuário do DB2 seja **mydb2id**.

  ```
  -W DBPassword.userID="mydb2id"
  ```


RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 1599
3698
Doc

- Especifique a senha do ID do usuário administrador do DB2 (**mydb2id**). Por exemplo, você deseja que a senha seja **mypass**.

  ```
  -W DBPassword.password="mypass"
  ```

- Especifique o nome do banco de dados que será criado e utilizado pelo IBM Tivoli Storage Area Network Manager. Por exemplo, você deseja que o nome do banco de dados seja **mydb**.

  ```
  _W SANPassword1.dbName="mydb"
  ```

- Especifique o ID do usuário do banco de dados que é diferente do ID do usuário administrativo do DB2. Por exemplo, você deseja utilizar **mydbuser**.

  ```
  -W SANPassword1.userID="mydbuser"
  ```

- Especifique uma senha para o ID do usuário do banco de dados (**mydbuser**). Por exemplo, você deseja utilizar a senha **mydbpass**.

  ```
  -W SANPassword1.password="mydbpass"
  ```

- Especifique um ID do usuário WebSphere. Por exemplo, você deseja utilizar **mywebid**.

  ```
  -W WASPassword.userID="mywebid"
  ```

- Especifique uma senha do ID do usuário WebSphere (**mywebid**). Por exemplo, você deseja utilizar **mywebpass**.

  ```
  -W WASPassword.password="mywebpass"
  ```

- Especifique uma senha para comunicações do gerenciador, agente e console. Por exemplo, você deseja utilizar **hostcomm**.

  ```
  -W comPassword.password="hostcomm"
  ```

- Especifique a letra da unidade em que o Tivoli NetView será instalado. Isto é requerido somente para o gerenciador do Windows. Por exemplo, você deseja instalar o Tivoli NetView na unidade E.

  ```
  -W beanNVDriveInput.chcDriveName="E"
  ```

- Especifique a senha do Tivoli NetView. Isto é requerido somente para o gerenciador do Windows. Por exemplo, você deseja utilizar **netviewpass**.

  ```
  -W beanNetViewPasswordPanel.password="netviewpass"
  ```

Como Instalar o Gerenciador

Para instalar o gerenciador do Windows utilizando o arquivo **manager.opt**, execute este comando:

```
setup -silent -options <install_dir>\manager.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

Para instalar o gerenciador do AIX utilizando o arquivo **manager.opt**, execute este comando:

```
setup.aix -silent -options <install_dir>/manager.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

O arquivo de opções do agente localiza-se no diretório de instalação do agente. O arquivo de opções chama-se **agent.opt**. Para poder instalar o agente, você deve alterar os parâmetros apropriados no arquivo de opções. Consulte Figura 161.

```
################################################################################
# InstallShield Options File Template for Agent silent install
#
# This file can be used to create an options file (i.e., response file) for the
# wizard "Setup". Options files are used with "-options" on the command line to
# modificar definições do assistente.
#
# The settings that can be specified for the wizard are listed below. To use
# this template, follow these steps:
#
#    1. Specify a value for a setting by replacing the characters 'value'.
#    Read each settings documentation for information on how to specify its
#    valor.
#
#    2. Save the changes to the file.
#
#    3. To use the options file with the wizard, specify -options filename
#    as a command line argument to the wizard, where filename is the name
#    deste arquivo de opções.
#    example:
#      setup.exe -silent -options agent.opt
#
#
################################################################################

#-------------------------------------------------------------------------------
# Select default language
# Example:
#  -P defaultLocale="English"
#-------------------------------------------------------------------------------
#-P defaultLocale="English"

#-------------------------------------------------------------------------------
# Installation destination directory:
#
# The install location of the product. Specify a valid directory into which the
# product should be installed. If the directory contains spaces, enclose it in
# double-quotes. For example, to install the product to C:\Program Files\My
# Produto no Windows, utilize
# -P installLocation="C:\Program Files\My Product"
#  -P installLocation="C:/tivoli/itsanm/agent"
# For Unix
#  -P installLocation="/tivoli/itsanm/agent"
#-------------------------------------------------------------------------------
-P installLocation="c:/tivoli/itsanm/agent"

#-------------------------------------------------------------------------------
# Specify full qualified name of remote manager machine:
# Example:
#  -W managerNamePort.managerName="manager.sanjose.ibm.com"
#-------------------------------------------------------------------------------
-W managerNamePort.managerName="manager.sanjose.ibm.com"
```

Figura 161. Arquivo Agent.opt (Parte 1 de 2)

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1600
3698
Doc.

```
#-------------------------------------------------------------------------------
# Specify base port number of remote manager:
# Example:
#  -W managerNamePort.managerPort=9550
#-------------------------------------------------------------------------------
-W managerNamePort.managerPort=9550

#-------------------------------------------------------------------------------
# Base port number for this installation
# Example:
#  -W portNoBean.portNumber=9570
#-------------------------------------------------------------------------------
-W portNoBean.portNumber=9570

#-------------------------------------------------------------------------------
# Manager, Agent, Console communication password
# Exemplo:
#  -W comPassword.password="password"
#-------------------------------------------------------------------------------
-W comPassword.password="password"

#-------------------------------------------------------------------------------
# Property use by installation program.  Do not remove or modify.
#-------------------------------------------------------------------------------
-W setWinDestinationBean.value="$P(installLocation)"
```

Figura 161. Arquivo Agent.opt (Parte 2 de 2)

Altere apenas os parâmetros listados a seguir. Não altere nenhum outro parâmetro.

- Especifique o diretório de destino de instalação. No Windows, para que o diretório de destino da instalação seja `C:/myagent/itsanm/agent`, insira o exemplo da seguinte forma:

  ```
  -P installLocation="C:/myagent/itsanm/agent"
  ```

  No agente UNIX, insira o exemplo da seguinte forma:

  ```
  -P installLocation="/myagent/itsanm/agent"
  ```

  Nota: Este procedimento aceita as barras normal e invertida para caminhos de diretórios em uma plataforma Windows.

- Especifique o nome completo da máquina do gerenciador remoto. Por exemplo, você deseja que o nome seja **mydivision.mycompany.com**.

  ```
  -W managerNamePort.managerName="mydivision.mycompany.com"
  ```

- Especifique o número da porta base da máquina do gerenciador remoto. Por exemplo, você deseja utilizar **9800**.

  ```
  -W managerNamePort.managerPort=9800
  ```

- Especifique o número da porta base para este host gerenciado. Por exemplo, você deseja que a base seja **9820**.

  ```
  -W portNoBean.portNumber=9820
  ```

- Especifique uma senha para comunicações do gerenciador, agente e console. Por exemplo, você deseja utilizar **hostcomm**.

  ```
  -W comPassword.password="hostcomm"
  ```

Como Instalar o Agente

Para instalar o agente do Windows utilizando o arquivo **agent.opt**, execute este comando:

```
setup -silent -options <install_dir>/agent.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

Para instalar o agente do AIX utilizando o arquivo **agent.opt**, execute este comando:

```
./setup.aix -silent -options <install_dir>/agent.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

Para instalar o agente do Solaris utilizando o arquivo **agent.opt**, execute este comando:

```
./setup.sol -silent -options <install_dir>/agent.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

Para instalar o agente do Linux utilizando o arquivo **agent.opt**, execute este comando:

```
./setup.lin -silent -options <install_dir>/agent.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

Instalando o Console Remoto

O arquivo de opções do console remoto localiza-se no diretório de instalação do console. O arquivo de opções chama-se **console.opt**. Para poder instalar o agente, você deve alterar os parâmetros apropriados no arquivo de opções. Consulte Figura 162 na página 196.

RQS nº 03/2005 - CN
Fls. Nº 1601
Doc: 3698

```
##############################################################################
# InstallShield Options File Template for Remote Console silent install
#
# This file can be used to create an options file (i.e., response file) for the
# wizard "Setup". Options files are used with "-options" on the command line to
# modificar definições do assistente.
#
# The settings that can be specified for the wizard are listed below. To use
# this template, follow these steps:
#
#    1. Specify a value for a setting by replacing the characters 'value'.
#    Read each settings documentation for information on how to specify its
#    valor.
#
#    2. Save the changes to the file.
#
#    3. To use the options file with the wizard, specify -options filename
#    as a command line argument to the wizard, where filename is the name
#    deste arquivo de opções.
#    exemplo:
#      setup.exe -silent -options console.opt
#
#
##############################################################################

#-----------------------------------------------------------------------------
# Select default language
# Example:
#  -P defaultLocale="English"
#-----------------------------------------------------------------------------
#-P defaultLocale="English"
```

Figura 162. Arquivo Console.opt (Parte 1 de 2)

```
#-------------------------------------------------------------------------------
# Installation destination directory.
#
# The install location of the product. Specify a valid directory into which the
# product should be installed. If the directory contains spaces, enclose it in
# double-quotes. For example, to install the product to C:\Program Files\My
# Produto no Windows, utilize
# -P installLocation="C:\Program Files\My Product"
#  -P installLocation="C:/tivoli/itsanm/console"
#-------------------------------------------------------------------------------
-P installLocation="c:/tivoli/itsanm/console"
#-------------------------------------------------------------------------------
# Specify full qualified name of remote manager machine:
# Exemplo:
#  -W beanManagerLocation.HostName="manager.sanjose.ibm.com"
#-------------------------------------------------------------------------------
-W beanManagerLocation.HostName="manager.sanjose.ibm.com"

#-------------------------------------------------------------------------------
# Specify base port number of remote manager:
# Exemplo:
#  -W beanManagerLocation.PortNo=9550
#-------------------------------------------------------------------------------
-W beanManagerLocation.PortNo=9550

#-------------------------------------------------------------------------------
# Base port number for this installation
# Exemplo:
#  -W portNoBean.portNumber=9560
#-------------------------------------------------------------------------------
-W portNoBean.portNumber=9560

#-------------------------------------------------------------------------------
# Manager, Agent, Console communication password
# Exemplo:
#  -W comPassword.password="password"
#-------------------------------------------------------------------------------
-W comPassword.password="password"

#-------------------------------------------------------------------------------
# Drive Letter where Netview to be installed.
# Exemplo:
#  -W beanNVDriveInput.chcDriveName="C"
#-------------------------------------------------------------------------------
-W beanNVDriveInput.chcDriveName="C"

#-------------------------------------------------------------------------------
# Netview password.
# Exemplo:
#  -W beanNetViewPasswordPanel.password="password"
#-------------------------------------------------------------------------------
-W beanNetViewPasswordPanel.password="password"
```

Figura 162. Arquivo Console.opt (Parte 2 de 2)

Altere apenas os parâmetros listados a seguir. Não altere nenhum outro parâmetro.

- Especifique o diretório de destino de instalação. Para que o diretório de destino da instalação seja `C:/myconsole/itsanm/console`, insira o exemplo da seguinte forma:

  ```
  -P installLocation="C:/myconsole/itsanm/console"
  ```

  Nota: Este procedimento aceita as barras normal e invertida para caminhos de diretórios em uma plataforma Windows.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1662
Doc. 3698

- Especifique o nome completo da máquina do gerenciador remoto. Por exemplo, você deseja que o nome seja **mydivision.mycompany.com**.

  ```
  -W beanManagerLocation.HostName="mydivision.mycompany.com"
  ```

- Especifique o número da porta base da máquina do gerenciador remoto. Por exemplo, você deseja utilizar **9800**..

  ```
  -W beanManagerLocation.PortNo=9800
  ```

- Especifique o número da porta base para este console. Por exemplo, você deseja que a base seja **9830**.

  ```
  -W portNoBean.portNumber=9830
  ```

- Especifique uma senha para comunicações do gerenciador, agente e console. Por exemplo, você deseja utilizar **hostcomm**.

  ```
  -W comPassword.password="hostcomm"
  ```

- Especifique a letra da unidade em que o Tivoli NetView será instalado. Isto é requerido somente para o gerenciador do Windows. Por exemplo, você deseja instalar o Tivoli NetView na unidade **E**.

  ```
  -W beanNVDriveInput.chcDriveName="E"
  ```

- Especifique a senha do Tivoli NetView. Por exemplo, você deseja utilizar **netviewpass**.

  ```
  -W beanNetViewPasswordPanel.password="netviewpass"
  ```

Como Instalar o Console Remoto

Para instalar o console remoto utilizando o arquivo **console.opt**, execute este comando:

```
setup -silent -options <install_dir>\console.opt
```

Onde *install_dir* é o diretório onde o arquivo de opções está localizado.

Desinstalando o IBM Tivoli Storage Area Network Manager

Esta seção descreve como desinstalar o IBM Tivoli Storage Area Network Manager se o produto foi instalado pela instalação silenciosa.

Removendo a Instalação do Gerenciador

Para desinstalar o gerenciador no Windows, siga esta etapa:

1. A partir do diretório de instalação, execute o seguinte comando:

   ```
   c:\tivoli\itsanm\manager\_uninst\uninstall -silent
   ```

Para desinstalar o gerenciador do AIX, siga esta etapa:

1. A partir do diretório de instalação, execute este comando:

   ```
   /tivoli/itsanm/manager/_uninst/uninstall -silent
   ```

Desinstalando Console Remoto

Para desinstalar o console remoto, siga esta etapa:

1. Execute este comando no diretório de instalação:

   ```
   c:\tivoli\itsanm\console\_uninst\uninstall -silent
   ```

Desinstalando os Agentes

Para desinstalar o agente do Windows, siga esta etapa:

1. A partir do diretório de instalação, execute este comando:

   ```
   c:\tivoli\itsanm\agent\_uninst\uninstall -silent
   ```

Para desinstalar o agente do UNIX, siga esta etapa:

1. A partir do diretório de instalação, execute este comando:
   `/tivoli/itsanm/agent/_uninst/uninstall -silent`

10100
A-

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1603
Nº 3698
Doc.

10099
A.

Apêndice B. Sugestões e Dicas

Esta seção fornece informações sobre os seguintes itens:

Tabela 16. Informações sobre Sugestões e Dicas para o Tivoli Storage Area Network Manager

Item	Consulte
Dicas sobre execução com o DB2	"Dicas sobre Execução com o DB2"
Como verificar um nome de host completo	"Verificando Nomes de Host Completos" na página 204
Como alterar o arquivo HOSTS	"Alterando o Arquivo HOSTS" na página 206
Como verificar um endereço IP estático	"Verificando um Endereço IP Estático" na página 207
Como alterar o nome da comunidade SNMP	"Alterando o Nome da Comunidade SNMP" na página 208
Dicas sobre execução com o Tivoli NetView	"Dicas sobre Execução com o Tivoli NetView" na página 209
Informações adicionais sobre o Tivoli Storage Area Network Manager	"Informações Adicionais" na página 210
Como Ativar a MIB de Gerenciamento de FC	"Ativando a MIB de Gerenciamento FC" na página 213
Classes de Eventos e Atributos do Tivoli Enterprise Console	"Classes de Eventos e Atributos do Tivoli Enterprise Console" na página 213

Dicas sobre Execução com o DB2

Esta seção fornece dicas sobre execução com o DB2.

Configurando o Banco de Dados DB2

O banco de dados DB2 aumentará de tamanho à medida em que as informações forem coletadas pelo IBM Tivoli Storage Area Network Manager. Para evitar ficar sem espaço, é recomendado seguir as etapas abaixo para configurar o banco de dados DB2.

Siga estas etapas:

1. Pare o gerenciador.

   Para parar o gerenciador no Windows, siga essas etapas:

   a. Na barra de ferramentas, clique no seguinte:

      ```
      Iniciar -> Configurações -> Painel de Controle ->
      Ferramentas Administrativas -> Serviços
      ```

   b. No painel Serviços, localize e realce **IBM WebSphere Application Server V5 – ITSANM – Manager**.

   c. Dê um clique com o botão direito do mouse em **IBM WebSphere Application Server V5 – ITSANM–Manager**.

   d. Clique em **Parar**.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1604
3698
Doc.

Para parar o gerenciador no AIX, vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

```
/tivoli/itsanm/manager/bin/aix/stopSANM.sh
```

2. Inicie um ambiente de DB2.

   No Windows, digite **db2cmd** em uma janela de prompt de comandos. É exibida uma nova janela db2cmd.

   No AIX, em um prompt do shell, execute o db2profile de seu proprietário de instância de DB2. Por exemplo, se o ID de proprietário da instância de DB2 for db2inst1, execute este comando:

   ```
   $ . ~/db2inst1/sqllib/db2profile
   ```

3. Execute os seguintes comandos. Esses exemplos utilizam o nome de banco de dados padrão, que é itsanmdb. Se o nome de seu banco de dados for diferente, utilize o nome de seu banco de dados.

   ```
   db2 update db cfg for itsanmdb using LOGFILSIZ 2500
   db2 update db cfg for itsanmdb using LOGPRIMARY 4
   db2 update db cfg for itsanmdb using LOGSECOND 20
   ```

4. Inicie novamente o gerenciador.

   No Windows, siga estas etapas:

   a. Na barra de ferramentas, clique no seguinte:

      ```
      Iniciar -> Configurações -> Painel de Controle ->
      Ferramentas Administrativas -> Serviços
      ```

   b. No painel Serviços, localize e realce **IBM WebSphere Application Server V5 – ITSANM – Manager**.

   c. Dê um clique com o botão direito do mouse em **IBM WebSphere Application Server V5 – ITSANM–Manager**.

   d. Dê um clique em **Iniciar**.

   No AIX, vá para o diretório de trabalho e execute este comando (utilizando o diretório padrão):

   ```
   /tivoli/itsanm/manager/bin/aix/startSANM.sh
   ```

Gerenciando os Logs de Transação

O banco de dados que é utilizado pelo gerenciador tem a opção de recuperação de banco de dados ativada, por padrão. Isso permite a recuperação do banco de dados em caso de falha do sistema. Ativando a opção de recuperação, o DB2 irá gerar logs de transação e salvá-los em um diretório do sistema do DB2. Com o tempo, esses logs aumentarão de tamanho. O modo recomendado para liberar espaço é utilizar a função **userexit** do DB2, conforme descrito no *Guia de Administração do DB2*. Outro modo de liberar espaço no sistema de arquivos é mover os logs inativos para outro sistema de arquivos. Este método é descrito abaixo. Para mover os logs inativos para outro sistema de arquivos, siga as etapas abaixo.

Siga estas etapas:

1. Inicie um ambiente de DB2.

   No Windows, abra uma janela de prompt de comandos. Digite **db2cmd**.

   No AIX, em um prompt do shell, execute o db2profile do proprietário de sua instância de DB2. Se o proprietário da instância de DB2 for db2inst1, digite o seguinte:

   ```
   $ . ~/db2inst1/sqllib/db2profile
   ```

2. Emita o seguinte comando. Este exemplo utiliza o nome padrão itsanmdb de banco de dados. Se você utiliza um nome de banco de dados diferente, utilize o nome de seu banco de dados.

   ```
   db2 get db cfg for itsanmdb
   ```

3. É exibida uma lista de sua configuração de banco de dados. Procure os valores **Path to log files** e **First active log file**. O valor **Path to log files** é onde os arquivos de log estão localizados. O valor **First active log file** indica o log ativo atual. O exemplo a seguir mostra essa saída.

   ```
   Path to log files       = C:\DB2\NODE0000\SQL00014\SQLOGDIR\
   First active log file   = S0000014.LOG
   ```

   No AIX, o caminho será: DB2/NODE0000/SQL00014/SQLOGDIR/. Você pode mover os arquivos, S0000001.LOG até S0000013.LOG para outro sistema de arquivos ou para backup e remover os arquivos de log para liberar espaço de log. (Não mova o arquivo de log ativo.)

Este é um método para gerenciamento rápido de seus logs de transação. Contudo, o modo recomendado para liberar espaço é utilizar o programa **userexit** do DB2.

Utilizando o DB2 no Windows

Esta seção fornece algumas dicas e sugestões para a utilização do DB2 no Windows.

Verificando o DB2

Para ver se o DB2 está ativo e em execução, siga estas etapas:

1. Clique no seguinte:

   ```
   Iniciar -> Programas -> DB2 for Windows NT
   -> Control Center
   ```

2. Você obterá um log em uma janela de diálogo. Insira o ID de administrador do DB2 e a senha e clique em **OK**.
3. Você verá a janela **DB2 Control Center** com o nome do host no qual o banco de dados DB2 está instalado.
4. Após a instalação do IBM Tivoli Storage Area Network Manager, será possível verificar se os bancos de dados DB2 estão criados como mostra a Figura 163 na página 204.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1605
Nº 3698
Doc.

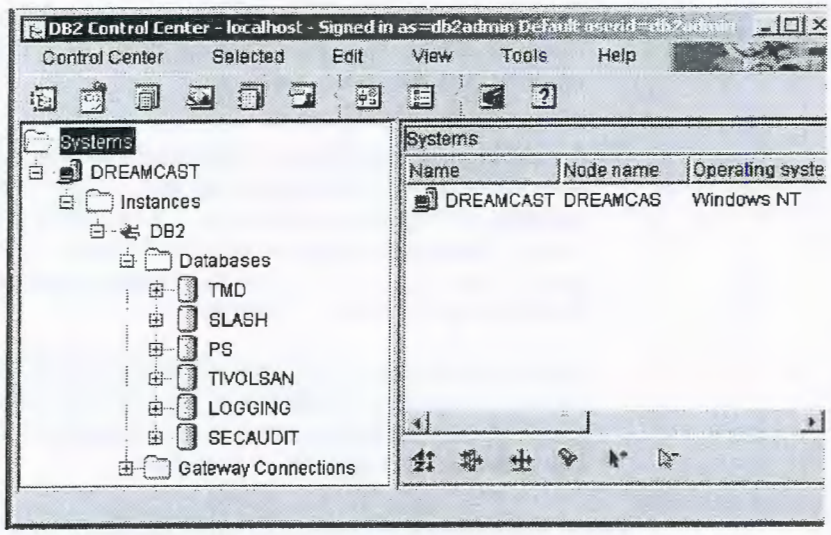


Figura 163. DB2 Control Center com DB2 Databases

Parando e Iniciando Novamente um Servidor DB2

Para abrir uma janela de comando do DB2, clique em:

```
Iniciar -> Programas
-> DB2 for Windows NT -> Command Window
```

Para parar o DB2, insira o seguinte comando na janela de comando do DB2: **db2stop**.

Para iniciar novamente o DB2, insira o seguinte comando na janela de comando do DB2: **db2start**.

Eliminando um Banco de Dados DB2

Para eliminar um banco de dados DB2, siga estas etapas:

1. Vá para o Centro de Controle DB2. Consulte "Utilizando o DB2 no Windows" na página 203.
2. Em Bancos de Dados DB2, clique com o botão direito do mouse no seu banco de dados (o exemplo na Figura 163 mostra TIVOLSAN). Clique em **Drop**. Um painel de confirmação é exibido. Clique em **OK**.

Utilizando o DB2 no AIX

Esta seção fornece algumas dicas e sugestões para a utilização do DB2 no AIX.

Para verificar se o DB2 está sendo executado, execute este comando:

```
ps -ef
```

Esse comando exibe os processos em execução.

Verificando Nomes de Host Completos

O IBM Tivoli Storage Area Network Manager exige nomes de host completos. Algumas máquinas podem estar configuradas para retornar um nome de host abreviado, como **ddunham**, em vez de um nome de host completo, como **ddunham.myorg.mycompany.com.**

Sistemas Windows 2000

Para verificar se um sufixo DNS (Domain Name System) primário está definido, siga estas etapas:

1. No desktop, clique com o botão direito do mouse em **Meu computador**.
2. Clique em **Propriedades**.
3. Clique na guia **Identificação de rede**.
4. Verifique se o campo **Nome completo do computador** contém um nome completo de domínio. Em caso negativo, siga estas etapas:
   a. Clique em **Propriedades** na guia **Identificação de rede**.
   b. Na janela Alterações de identificação, clique em **Mais**.
   c. No campo **Sufixo DNS primário deste computador**, digite o sufixo DNS primário e, quando solicitado, inicie novamente o computador.

Sistemas Windows NT

Para verificar se um sufixo DNS primário está definido, siga estas etapas:

1. Na barra de tarefas do Windows, clique em **Iniciar** → **Configurações** → **Painel de Controle**.
2. Na janela Painel de Controle, dê um clique duplo em **Rede**.
3. Clique na guia **Protocolos**.
4. Selecione o protocolo TCP/IP e clique em **Propriedades**.
5. Clique na guia **DNS**.
6. Verifique se o campo **Domínio** contém um sufixo de domínio. Em caso negativo, digite o sufixo, clique em **OK** e, quando solicitado, inicie novamente o computador.

Sistemas AIX

A ordem de pesquisa de nomes de domínio padrão é a seguinte:

1. Servidor DNS (Domain Name System)
2. NIS (Network Information Service)
3. Arquivo `/etc/hosts` local

Se o arquivo `/etc/resolv.conf` não existir, o arquivo `/etc/hosts` será utilizado. Se apenas o arquivo `/etc/hosts` for utilizado, o nome completo do computador deverá ser o primeiro nome listado após o endereço IP.

Verifique se o arquivo `/etc/resolv.conf` existe e se contém as informações apropriadas, como:

```
domínio minhadivisão.minhaempresa.com
servidordenomes 123.123.123.123
```

Se o NIS estiver instalado, o arquivo `/etc/irs.conf` substituirá o padrão do sistema. Essa variável contém as seguintes informações:

```
hosts = bind,local
```

O arquivo `/etc/netsvc.conf`, se houver, substituirá o arquivo `/etc/irs.conf` e o padrão do sistema. Essa variável contém as seguintes informações:

```
hosts = bind,local
```

Se a variável de ambiente NSORDER estiver definida, substituirá todos os arquivos precedentes. Essa variável contém as seguintes informações:

```
export NSORDER=bind,local
```


10095 A
ROS nº 03/2003
CPMI — CORREIOS
Fls. Nº 1666
3698
Doc.

Sistemas Solaris

Verifique se o arquivo /etc/resolv.conf existe e se contém as informações apropriadas, como:

```
domínio minhadivisão.minhaempresa.com
servidordenomes 123.123.123.123
```

Um nome abreviado será utilizado se o arquivo /etc/nsswitch.conf contiver uma linha iniciada conforme mostrado a seguir e se o arquivo /etc/hosts contiver o nome abreviado para o computador:

```
hosts: files
```

Para corrigir esse problema, siga estas etapas:

1. Altere a linha no arquivo /etc/nsswitch.conf para o seguinte:

   ```
   hosts: dns nis files
   ```

2. Insira o seguinte comando para parar o serviço inet:

   ```
   /etc/init.d/inetsvc stop
   ```

3. Insira o seguinte comando para iniciar novamente o serviço inet:

   ```
   /etc/init.d/inetsvc start
   ```

Sistemas Linux

Execute este comando para exibir o nome completo do host do computador:

```
more /etc/hosts
```

É exibido um exemplo da saída:

```
123.123.123.123 mydivision.mycompany.com short_name
```

O endereço IP é exibido seguido do nome completo e do nome resumido do host.

Alterando o Arquivo HOSTS

Ao instalar o Service Pack 3 para o Windows 2000 nos computadores, você deverá seguir estas etapas para evitar problemas de endereçamento com o Tivoli Storage Area Network Manager. O problema é causado pelo protocolo de resolução de endereços, que retorna o nome abreviado (nome do host incompleto). É possível evitá-lo alterando as entradas nas tabelas de host correspondentes no servidor DNS e no computador local. O nome do host completo deve estar listado antes do nome abreviado.

Para corrigir esse problema, siga estas etapas:

1. Você localizará o arquivo HOSTS no diretório %SystemRoot%\system32\drivers\etc\.
2. Será necessário editar esse arquivo HOSTS.Um exemplo de arquivo HOSTS está exibido a seguir.

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
```

```
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

192.168.123.146     jason     jason.groupa.mycompany.com
```

3. Insira o nome do host completo como a primeira linha a ser pesquisada na tabela. (As linhas precedidas pelo sinal # são linhas de comentário.) Por exemplo, inclua a linha realçada em negrito no arquivo:

```
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

192.168.123.146     jason.groupa.mycompany.com      jason
192.168.123.146     jason     jason.groupa.mycompany.com
```

Nota: Nomes de host fazem distinção entre maiúsculas e minúsculas. Essa é uma limitação do WebSphere. Verifique o nome do host. Consulte "Etapa 2: Verificar o Nome do Computador" na página 21. Por exemplo, se o computador mostrar o nome como JASON (letras maiúsculas), será necessário inserir JASON no arquivo HOSTS.

Verificando um Endereço IP Estático

O IBM Tivoli Storage Area Network Manager (componente gerenciador) deve possuir um endereço IP estático. O servidor DNS remoto deve conhecer o endereço IP estático de cada máquina.

Para o Windows 2000: Para localizar o endereço IP estático, execute as etapas a seguir:

1. Clique com o botão direito do mouse em **Meus locais de rede**.
2. Selecione **Propriedades**.
3. Clique com o botão direito do mouse em **Conexão de rede local**.
4. Selecione **Propriedades**.
5. Selecione **Protocolo Internet (TCP/IP)**.
6. Clique em **Propriedades**.
7. A janela **Propriedades de Protocolo Internet (TCP/IP)** é exibida.

10093 A-

CPMI - CORREIOS
Fls Nº 1607
Nº 3698
Doc.

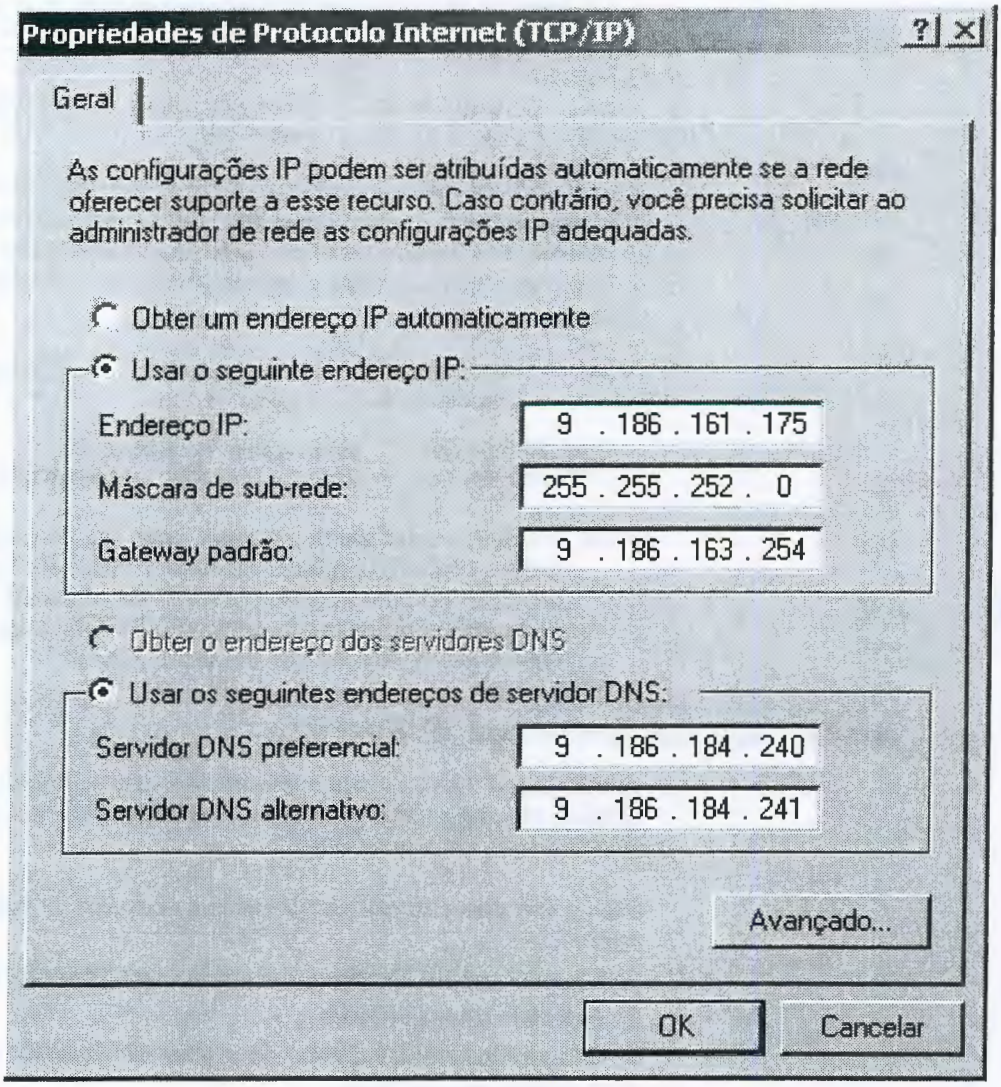


Figura 164. Janela Propriedades de Protocolo Internet (TCP/IP)

Se a opção Usar o seguinte endereço IP estiver selecionada, significa que você possui um endereço IP estático.

Alterando o Nome da Comunidade SNMP

O valor padrão do nome da comunidade SNMP é PUBLIC.

Nota: O IBM Tivoli Storage Area Network Manager oferece suporte para apenas um nome de comunidade SNMP. Um comutador pode ter vários nomes de comunidade, mas o IBM Tivoli Storage Area Network Manager somente pode se comunicar com um desses nomes. Além disso, se o nome da comunidade SNMP inserido no comando não for um nome de comunidade no comutador, as consultas SNMP do IBM Tivoli Storage Area Network Manager atingirão o tempo limite. O IBM Tivoli Storage Area Network Manager não poderá se comunicar com o comutador.

Se você quiser alterar o nome da comunidade, siga estas etapas:

1. Abra uma janela de prompt de comandos na máquina do gerenciador.

10091
A.

2. Altere para o seguinte diretório:

   ```
   tsnm\manager\bin\w32-ix86
   ```

3. Insira os seguintes comandos:

   ```
   setenv
   srmcp -u ID_do_usuário -p senha ConfigService set SnmpCommunityName nome
   ```

   Em que:
   - *ID_do_usuário* é o ID do usuário
   - *senha* é a senha do usuário
   - *nome* é o nome da comunidade

Dicas sobre Execução com o Tivoli NetView

Esta seção descreve como iniciar um aplicativo a partir do Console do IBM Tivoli Storage Area Network Manager.

Como Ativar um Aplicativo a partir do Console Remoto

Os dispositivos que iniciam seus próprios aplicativos de gerenciamento em vez de utilizarem uma interface da Web ou Telnet devem ter a variável de ambiente PATH definida. A variável PATH deve ser definida como a localização do aplicativo. Se você não defini-la, obterá um erro de aplicativo não encontrado ao tentar iniciar o aplicativo de gerenciamento para o dispositivo.

Para definir a variável PATH, siga estas etapas:

1. No desktop, clique com o botão direito do mouse em **Meu computador**.
2. Selecione **Propriedades**.
3. Selecione a guia **Avançado** → **Variáveis de ambiente**.
4. Em **Variáveis do sistema**, selecione **PATH**.
5. Edite a variável PATH para incluir a localização do aplicativo.

Como Verificar o Daemon do NetView

Se você quiser verificar se o daemon do NetView está em execução, siga estas etapas:

1. No menu principal do Tivoli NetView, clique em **Options**.
2. Selecione **Server Setup**.
3. A caixa de diálogo Server Setup é exibida. Clique na guia **Daemons**.

RQS nº 03/2005 - CN
CORREIOS
Fls Nº 1608
3698
Doc.

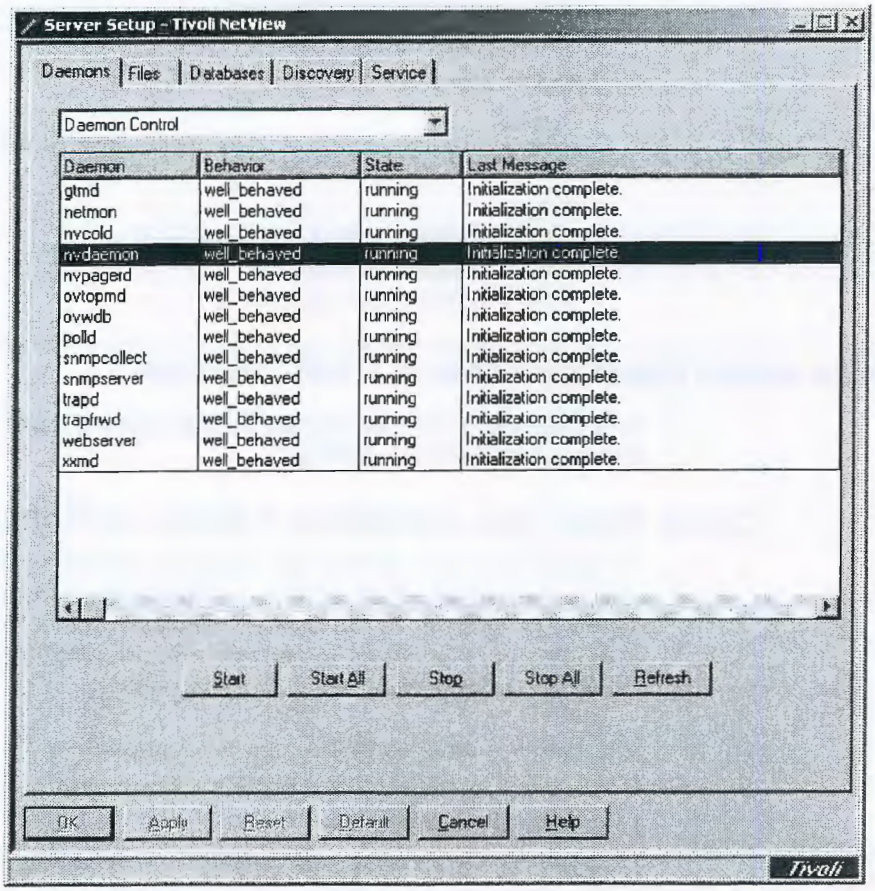


Figura 165. Caixa de Diálogo Server Setup

A coluna Estado indica se o daemon do NetView (**nvdaemon**) está ou não em execução.

Para parar o daemon NetView, realce **nvdaemon** e clique em **Stop**.

Para iniciar o daemon NetView, realce **nvdaemon** e clique em **Start**.

Informações Adicionais

Esta seção fornece informações adicionais sobre a operação do IBM Tivoli Storage Area Network Manager.

Como o Tivoli Storage Area Network Manager Utiliza Eventos em Banda e Traps SNMP Fora de Banda

O Tivoli Storage Area Network Manager utiliza eventos em banda e traps SNMP fora de banda para iniciar uma operação de descoberta na SAN.

Eventos em banda e traps SNMP fornecem as mesmas informações, como uma alteração ocorrida na SAN indicando que uma operação de descoberta deve ser executada. Eventos em banda e traps SNMP permitem que o Tivoli Storage Area Network Manager saiba o momento em que algo ocorreu na SAN e, em seguida, que uma operação de descoberta foi executada para identificar as alterações. Os agentes do Tivoli Storage Area Network Manager em execução nos hosts

gerenciados detectam eventos em banda. O agente de alteração fora de banda do Tivoli Storage Area Network Manager detecta os traps SNMP. Para que o Tivoli Storage Area Network Manager receba os traps SNMP, configure o dispositivo, como um comutador, para enviar traps ao Tivoli Storage Area Network Manager (servidor de gerenciamento).

O Tivoli Storage Area Network Manager descobre as informações sobre a SAN desempenhando as seguintes operações:

- Comunica-se com os agentes do Tivoli Storage Area Network Manager. Os agentes são executados nos hosts gerenciados (descoberta em banda).
- Envia consultas MIB (Management Information Base) diretamente a comutadores e outros dispositivos (descoberta fora de banda).

As informações sobre hosts e dispositivos são reunidas pela operação em banda. As informações sobre topologia são reunidas com o uso da operação de descoberta em banda e/ou fora de banda. Essas duas operações de descoberta da topologia fornecem o mesmo nível de informações. Entretanto, as informações sobre zonas somente estão disponíveis por meio da operação de descoberta em banda. O uso simultâneo de operações de descoberta em banda e fora de banda estende a faixa de dispositivos suportados pelo Tivoli Storage Area Network Manager. Alguns comutadores somente oferecem suporte para o mecanismo em banda, enquanto outros somente oferecem suporte para o mecanismo fora de banda.

Se não houver agentes em execução nos sistemas host, será possível utilizar as operações de descoberta fora de banda e a monitoração de traps SNMP para monitorar a SAN. Nessa configuração, o console do Tivoli Storage Area Network Manager somente pode indicar informações em nível de conexão e comutador. Os dispositivos e hosts serão exibidos como entidades desconhecidas. Você pode alterar o ícone e os rótulos dessas entidades desconhecidas para algo mais apropriado à sua empresa. Se quiser utilizar o Tivoli Storage Area Network Manager dessa maneira, configure-o para receber traps SNMP. Os traps SNMP determinam quando iniciar uma operação de redescoberta. Considere essa configuração se as seguintes condições forem verdadeiras:

- Você deseja incluir sistemas não suportados na SAN
- Você deseja monitorar máquinas sobre as quais não possui controle direto.

Os traps SNMP enviados pelos dispositivos e pelo Tivoli Storage Area Network Manager podem ser enviados ao Console do Tivoli Storage Area Network Manager. Os eventos podem ser exibidos no navegador de eventos ou enviados a outro console de traps para monitoração. Em seguida, você pode providenciar uma recuperação após erros ou outro processamento avançado, como a paginação.

A tabela a seguir mostra os tipos de informações reunidas para operações de descoberta em banda e fora de banda. Os mecanismos de varredura de topologia e atributo são executados quando possível. Por exemplo, se uma varredura em banda for executada, informações sobre topologia e atributo serão reunidas caso seja possível. Essa tabela também mostra quais informações serão reunidas se apenas uma varredura de topologia ou atributo for executada.

10089 A
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1609
3698
Doc.

Tabela 17. Informações Reunidas pelo Tivoli Storage Area Network Manager

Tipos de Informações	Somente Varredura em Banda	Somente Varredura Fora de Banda	Varreduras em Banda e Fora de Banda
Topologia	• Comutadores e conexões • Informações sobre zonas • Hosts e dispositivos são exibidos como entidades desconhecidas	• Comutadores e conexões • Hosts e dispositivos são exibidos como entidades desconhecidas	• Comutadores e conexões • Informações sobre zonas • Hosts e dispositivos são exibidos como entidades desconhecidas
Atributo	• Identificar hosts • Identificar dispositivos de nó de extremidade • Informações centralizadas em dispositivo e centralizadas em host	• —	• Identificar hosts • Identificar dispositivos de nó de extremidade • Informações centralizadas em dispositivo e centralizadas em host
Topologia e atributo	• Comutadores e conexões • Informações sobre zonas • Identificar hosts • Identificar dispositivos de nó de extremidade • Informações centralizadas em dispositivo e centralizadas em host	• Comutadores e conexões • Hosts e dispositivos são exibidos como entidades desconhecidas	• Comutadores e conexões • Informações sobre zonas • Identificar hosts • Identificar dispositivos de nó de extremidade • Informações centralizadas em dispositivo e centralizadas em host

Informações Coletadas com o Uso de Comutadores e HBAs de Fornecedores

A tabela a seguir mostra as informações coletadas com o uso de comutadores e HBAs de fornecedores. Essa tabela assume que os comutadores de fornecedores oferecem suporte para descoberta fora de banda. O RNID (Request Node Identification Data) é um ELS (Extended Link Service) de Canal de Fibra especificado no padrão FC-FS (Fibre Channel Framing and Signaling). O RNID ELS permite que uma porta envie solicitações a outras portas para reunir informações. Essas informações, como informações sobre tipos (HBA, comutador, dispositivo de armazenamento e assim por diante), são reunidas com o uso do protocolo de Canal de Fibra.

Tabela 18. Informações Reunidas pelo Tivoli Storage Area Network Manager com o Uso de Comutadores e HBAs de Fornecedores

Nível de Informações Coletadas	Nível de Suporte para Drivers de Dispositivos HBA de Fornecedores	Quais Informações Podem Ser Reunidas e Mostradas
Bom	Sem utilizar uma API comum	O Tivoli Storage Area Network Manager pode executar o gerenciamento fora de banda nessa situação. Além disso, se outros agentes em banda possuírem níveis melhores ou máximos de HBAs, o Tivoli Storage Area Network Manager poderá executar descoberta em banda por meio desses agentes. Informações mostradas: • Comutadores com conexões IP com o gerenciador. • Topologia que pode ser visualizada a partir dos comutadores com conexões IP com o gerenciador. • Hosts e outros dispositivos mostrados como entidades desconhecidas na exibição da topologia.

Tabela 18. Informações Reunidas pelo Tivoli Storage Area Network Manager com o Uso de Comutadores e HBAs de Fornecedores (continuação)

Nível de Informações Coletadas	Nível de Suporte para Drivers de Dispositivos HBA de Fornecedores	Quais Informações Podem Ser Reunidas e Mostradas
Melhor	Utiliza uma API comum sem o suporte do RNID	O Tivoli Storage Area Network Manager pode executar o gerenciamento fora de banda e em banda nessa situação. Outros agentes em banda não poderão obter informações RNID a partir desse HBA. Além do nível satisfatório de informações, você visualizará: • Hosts gerenciados com agentes instalados (não mostrados como entidades desconhecidas na exibição da topologia). • Alguns dispositivos de armazenamento não serão mais exibidos como entidades desconhecidas na exibição da topologia.
Máximo	API comum com suporte do RNID	Existe suporte total para informações fora de banda, em banda e RNID. Além do nível satisfatório e melhor de informações, você visualizará: • Todos os hosts gerenciados contendo HBAs que respondem ao RNID. Mesmo que o agente não esteja instalado, esses hosts não serão mostrados como entidades desconhecidas na exibição da topologia. • Os dispositivos de armazenamento que respondem ao RNID também não serão mais mostrados como entidades desconhecidas na exibição da topologia.

Ativando a MIB de Gerenciamento FC

Quando você tiver um comutador do tipo Brocade 2400 ou 2800, deverá ativar a MIB de gerenciamento FC no comutador. Para ativar o comutador, siga estas etapas:

1. Utilize Telnet para o comutador.
2. Efetue login.
3. No prompt, insira **snmpmibcapset**.
4. Certifique-se que a MIB de gerenciamento FC esteja marcada como **sim** para ser ativada. Caso contrário, digite **yes** e continue.
5. Não é necessário reinicializar o comutador neste ponto.

Classes de Eventos e Atributos do Tivoli Enterprise Console

As classes de eventos e atributos do Tivoli Enterprise Console aparecem na Tabela 19 na página 214.

RQS nº 03/2005
Fls. Nº 1610
3698
Doc.

Tabela 19. Classes de Eventos e Atributos do Tivoli Enterprise Console

Classe de Eventos	Atributos da Classe de Eventos
SANManagerEvent – esta classe herda seus atributos da classe de EVENTOS base e conseqüentemente inclui os atributos mostrados. Todas as classes restantes nessa tabela herdam os atributos desta classe e assim conterão esses atributos além daqueles exclusivos para cada classe de eventos específica.	**EventClass** A classe de eventos. **HostName** Nome do sistema no qual ocorre o evento. **Origem** O endereço IP do sistema host no qual ocorre o evento. **Origem** A origem do evento. Uma origem é um recurso do aplicativo ou do sistema. A origem deste programa é "Tivoli Storage Area Network Manager". **Suborigem** Uma classificação adicional da origem. **Mensagem** Um resumo em texto do evento. **MessageID** O ID da mensagem. **Gravidade** A gravidade do evento. Os diferentes tipos de gravidade estão definidos na classe do utilitário. Os níveis de gravidade predefinidos, em ordem de gravidade decrescente, são: FATAL, CRÍTICO, SECUNDÁRIO, AVISO, INOFENSIVO E DESCONHECIDO.

Tabela 19. Classes de Eventos e Atributos do Tivoli Enterprise Console (continuação)

Classe de Eventos	Atributos da Classe de Eventos
PhysicalEntityEvent – um evento que indica que ocorreu uma alteração relativa a um dispositivo físico. **Nota:** PhysicalEntityEvents derivam-se de EntityEvents que, por sua vez, derivam-se de SANManagerEvents. Os atributos listados são EntityEvent.	**UniqueId** Identifica exclusivamente uma linha em uma coluna do banco de dados. **EntityType** Identifica a coluna na tabela do banco de dados que contém informações sobre a entidade a que se destina esse evento. **Rótulo** É o nome inserido manualmente no console deste dispositivo em particular. Se nenhum nome inserido manualmente estiver disponível, será utilizado o nome relatado pelo agente de descoberta. Se nenhum deles estiver disponível, o WWN será utilizado. **Tipo** É o valor de tipo retornado pelos agentes de descoberta. Um exemplo de nó descoberto seria "Controlador Interno". **HighLevelDevice** Identifica o dispositivo em que a entidade física está contida. Por exemplo, o HLD de uma porta em uma chave poderia ser o nome da chave e o número da porta física da porta. **Estado** Este valor é recuperado do banco de dados e reflete o estado da entidade para a qual o evento foi enviado. O valor será "faltando" ou "normal". **EventType** Indica o tipo de evento. Os valores de exemplos são: "novo evento de dispositivo", "faltando evento de dispositivo" ou "evento de atributo modificado."

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1611
3698
Doc.

Tabela 19. Classes de Eventos e Atributos do Tivoli Enterprise Console (continuação)

Classe de Eventos	Atributos da Classe de Eventos
PhysicalRelationshipEvent – um evento que indica que ocorreu uma alteração relativa a um relacionamento entre as duas entidades físicas. As entidades são referidas como "ToObject" e "FromObject". **Nota:** PhysicalRelationshipEvents derivam-se de RelationshipEvents que, por sua vez, derivam-se de SANManagerEvents. Os atributos listados são RelationshipEvents.	**UniqueId** Identifica exclusivamente a linha na tabela do banco de dados que contém informações relativas à entidade para a qual recebemos esse evento. **EntityType** Identifica a tabela do banco de dados que contém informações sobre a entidade de relacionamento a que se destina esse evento. **ToObjectUniqueId** Identifica exclusivamente a linha na tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **ToObjectLabel** Este é o nome inserido manualmente, nome descoberto ou WWN do "ToObject". **ToObjectType** Identifica a tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **ToHighLevelDevice** Identifica o dispositivo que contém o "ToObject". Por exemplo, em um evento de relacionamento de uma entidade PortToPort, isto identificaria o dispositivo em que "to port" está: por exemplo, switch6a. **FromObjectUniqueId** Identifica exclusivamente a linha na tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **FromObjectLabel** Este é o nome inserido manualmente, nome descoberto ou WWN do "ToObject". **FromObjectType** Identifica a tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **FromHighLevelDevice** Identifica o dispositivo que contém o "FromObject". **Estado** Este valor é recuperado do banco de dados e reflete o estado da entidade de relacionamento para a qual o evento foi enviado. O valor será "faltando" ou "normal". **EventType** Indica a razão pela qual o evento foi enviado. Os valores de exemplos são: "novo evento de dispositivo", "faltando evento de dispositivo", "evento de atributo modificado."

10083
LA

Tabela 19. Classes de Eventos e Atributos do Tivoli Enterprise Console (continuação)

Classe de Eventos	Atributos da Classe de Eventos
LogicalEntityEvent – um evento que indica que ocorreu uma alteração relativa a uma entidade lógica. **Nota:** LogicalEntityEvents derivam-se de EntityEvents que, por sua vez, derivam-se de SANManagerEvents. Os atributos listados são EntityEvent.	**UniqueId** Identifica exclusivamente uma linha em uma coluna do banco de dados. **EntityType** Identifica a coluna na tabela do banco de dados que contém informações sobre a entidade a que se destina esse evento. **Rótulo** É o nome inserido manualmente no console desta entidade em particular. Se nenhum nome inserido manualmente estiver disponível, será utilizado o nome relatado pelo agente de descoberta. Se nenhum deles estiver disponível, o WWN será utilizado. **Tipo** É o valor de tipo retornado pelos agentes de descoberta. **HighLevelDevice** Identifica o dispositivo em que a entidade lógica está contida. Por exemplo, o HLD de uma porta poderia ser a chave e o número da porta física da porta. **Estado** Este valor é recuperado do banco de dados e reflete o estado da entidade para a qual o evento foi enviado. O valor será "faltando" ou "normal". **EventType** Indica a razão pela qual o evento foi enviado. Os valores de exemplos são: "novo evento de dispositivo", "faltando evento de dispositivo" ou "evento de atributo modificado."

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1612
3698
Doc.

10082
A.

Tabela 19. Classes de Eventos e Atributos do Tivoli Enterprise Console (continuação)

Classe de Eventos	Atributos da Classe de Eventos
LogicalRelationshipEvent – Um evento que indica que ocorreu uma alteração relativa a um relacionamento entre as duas entidades lógicas ou uma entidade física. As entidades são referidas como "ToObject" e "FromObject". **Nota:** LogicalRelationshipEvents derivam-se de RelationshipEvents que, por sua vez, derivam-se de SANManagerEvents. Os atributos listados são RelationshipEvents.	**UniqueId** Identifica exclusivamente a linha na tabela do banco de dados que contém informações relativas à entidade para a qual recebemos esse evento. **EntityType** Identifica a tabela do banco de dados que contém informações sobre a entidade de relacionamento a que se destina esse evento. **ToObjectUniqueId** Identifica exclusivamente a linha na tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **ToObjectLabel** Este é o nome inserido manualmente, nome descoberto ou WWN do "ToObject". **ToObjectType** Identifica a tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **ToHighLevelDevice** Identifica o dispositivo que contém o "ToObject". Por exemplo, em um evento de relacionamento de uma entidade PortToPort, isto identificaria o dispositivo em que "to port" está, por exemplo, switch6a. **FromObjectUniqueId** Identifica exclusivamente a linha na tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **FromObjectLabel** Este é o nome inserido manualmente, nome descoberto ou WWN do "ToObject". **FromObjectType** Identifica a tabela do banco de dados que contém informações relativas à "ToObject" deste evento de relacionamento. **FromHighLevelDevice** Identifica o dispositivo que contém o "FromObject". **Estado** Este valor é recuperado do banco de dados e reflete o estado da entidade de relacionamento para a qual o evento foi enviado. O valor será "faltando" ou "normal". **EventType** Indica a razão pela qual o evento foi enviado. Os valores de exemplos são: "novo evento de dispositivo", "faltando evento de dispositivo", "evento de atributo modificado."
SANManagerStatusEvent – eventos do produto Try and Buy ou quando Limpar Alterações é concluído.	**ActionPerformed** A ação executada para este evento.

10081
A-

Tabela 19. Classes de Eventos e Atributos do Tivoli Enterprise Console (continuação)

Classe de Eventos	Atributos da Classe de Eventos
SANRegionEvent – eventos relacionados a uma alteração na SAN ou zona.	**SANName** O nome da SAN. **ZoneName** O nome da zona. **Estado** Origina-se nas tabelas do banco de dados e teria um valor "faltando" ou "normal". **EventType** Indica a razão pela qual o evento foi enviado.
ServiceEvent – eventos relacionados a um início ou uma parada do serviço IBM Tivoli Storage Area Network Manager.	**ServiceName** O nome do serviço. **ServiceState** O estado do serviço.

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 1613
3698
Doc.

Apêndice C. Detecção de Problemas

A seção contém informações sobre resolução de problemas e como recuperar-se de uma condição de erro. Para obter mais informações, consulte:

- Documentação do DB2 no CD-ROM do DB2.
- Documentação do Tivoli NetView.

Detectando Problemas do Tivoli NetView

Tabela 20. Problemas do Tivoli NetView

Problema	Recuperação
Se você receber a seguinte mensagem de erro: `Tivoli NetView has determined that the SNMP service is not available. Please install this service before continuing.` O Serviço SNMP não foi instalado.	Instale o Serviço SNMP. Consulte "Etapa 5: Instale o Serviço SNMP" na página 29.
Se você receber a seguinte mensagem de erro: `O ID do usuário ou a senha inseridos para o endereço de destino do agente fora de banda <endereço_de_destino> estão incorretos.`	Um scanner fora de banda encontrou um erro ao tentar utilizar o ID do usuário ou a senha inseridos para o endereço de destino do agente fora de banda. Insira o ID do usuário ou a senha correto para o endereço de destino. Consulte "Configurando os Agentes Fora de Banda" na página 112. Se o problema continuar, entre em contato com o suporte ao cliente IBM.

Detectando Problemas do IBM Tivoli Storage Area Network Manager

Tabela 21. Problemas do Tivoli Storage Area Network Manager

Problema	Recuperação
O Tivoli Storage Area Network Manager não consegue criar o banco de dados itsanmdb.	Se você possui um banco de dados denominado itsanmdb e ele não está no formato aceitável para o Tivoli Storage Area Network Manager, a instalação será parada porque não é possível recriar o banco de dados itsanmdb. Supõe-se que você utilizará o nome do banco de dados padrão itsanmdb. O programa de instalação remove todos os componentes instalados. Você pode eliminar ou renomear o banco de dados itsanmdb por meio do DB2 no console do DB2. Se você não conseguir eliminar o banco de dados itsanmdb, siga estas etapas no console do DB2 no Windows: 1. Crie o catálogo do banco de dados. 2. Elimine o banco de dados itsanmdb. 3. Remova o catálogo do banco de dados. 4. Reinstale o Tivoli Storage Area Network Manager.
Você recebe a mensagem de erro: `JVM not found`	É necessário verificar se existe espaço temporário em disco suficiente para instalar o gerenciador, o host gerenciado e o console remoto do IBM Tivoli Storage Area Network Manager. Consulte Tabela 4 na página 10.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1614
3698
Doc.

Tabela 21. Problemas do Tivoli Storage Area Network Manager (continuação)

Problema	Recuperação
O console remoto não está funcionando e existem erros de conexão DB no log desse console remoto.	Isso pode ser causado pelo uso de um nome de host abreviado para o servidor DB. O servidor DB deve ter um nome de host completo. Verifique se o URL do DB no arquivo de propriedades pode ser resolvido no console remoto. Para verificar isso, insira um ping a partir do console remoto. Consulte "Etapa 3: Alterar o Arquivo HOSTS" na página 22.
A topologia não é atualizada após um disco ser removido ou incluído em um JBOD.	Um comutador pode não gerar um evento para notificar o IBM Tivoli Storage Area Network Manager sobre a remoção ou adição. A topologia pode não ser atualizada neste caso. No entanto, o comutador pode enviar uma notificação se estiver executando outra atividade e perceber que o disco foi incluído ou removido. Isso é específico para dispositivos de loop arbitrados.

Você recebe a mensagem de erro:
`BTATG0004I A GUID already exists on this host. A new GUID will not be created.`
	Restaram alguns arquivos na máquina após a remoção da instalação de um GUID Tivoli. Esses arquivos não devem afetar as operações do IBM Tivoli Storage Area Network Manager. Alguns exemplos de arquivos deixados na máquina são:
	`70 Aug 5 17:24 TIVGUID`
	`259 Aug 5 17:23 K90itsrm_agent`
	`265 Aug 5 17:23 S90itsrm_agent`

Você recebe a mensagem de erro:
`"Unable to invoke outband scan" on an IP address that is not on a SAN`
 	
ou
`BTAQE1112E During an outband scan, the scanner was unable to identify the target host.`
	Para exibir os eventos do sensor para um comutador que apenas é descoberto por meio do processo de discovery em banda, o nome especificado para o comutador deve corresponder ao nome abreviado utilizado para identificar esse comutador na rede IP. Entre em contato com o fabricante do comutador para obter informações sobre como configurar esse campo.

Após a configuração de um agente fora de banda e a definição do nome de usuário e da senha para comutadores Brocade SNMP fora de banda, a seguinte mensagem de aviso é exibida nos consoles telnet desses Comutadores Brocade. Esta mensagem será exibida nos consoles telnet para os quais as informações corretas de login foram inseridas, uma vez para cada processo de discovery : `Current Zoning Transaction was aborted. Reason code = Unknown (0)`	Esse é o comportamento esperado e é gerado pelo comutador. Não é necessária nenhuma ação do usuário. O Tivoli Storage Manager for SAN Management trava a transação de Zonas no comutador antes de ler os dados de zonas a partir desse comutador. Essa trava é liberada após a operação de leitura ser executada. A mensagem de aviso que indica que a transação de Zoneamento foi liberada é exibida nesse momento, no console do comutador.
Você não consegue parar um daemon de agente.	Certifique-se de que um processo de evento, topologia ou atributo não esteja em execução antes de parar o agente.
Você recebe a mensagem de erro: `Sending RNID command to device that does not support RNID.`	Um comando RNID foi enviado a um dispositivo que não oferece suporte para o RNID. Essas mensagens são informativas e podem ser ignoradas.

10078
A.

Tabela 21. Problemas do Tivoli Storage Area Network Manager (continuação)

Problema	Recuperação
O processo discovery fora de banda não está trabalhando com um comutador Brocade 2400/2800 ou IBM 2109.	É possível que a MIB FA (também conhecida como FC Management) MIB não foi ativada no comutador. Para verificar e ativar, siga estas etapas: 1. Utilize Telnet para o comutador. 2. Efetue login. 3. No prompt, insira **snmpmibcapset**. 4. Certifique-se que a MIB FA esteja marcada como **sim** para ser ativada. Caso contrário, digite **yes** e continue. 5. Não é necessário reinicializar o comutador neste momento.
Ao instalar o gerenciador do Windows, você recebe uma mensagem dizendo que o arquivo datastore.properties foi modificado. O programa perguntará se você deseja excluir ou não o arquivo. Responda "Yes, delete it".	A instalação falhou. Procure nos logs de instalação o motivo da falha.

ECT nº 03/2005
CPMI - CORREIOS
Fls Nº 1615
3698
Doc.

00077
A-

Apêndice D. Acessibilidade

Os recursos de acessibilidade ajudam os usuários com deficiências físicas, como movimentos restritos ou visão limitada, a utilizar produtos de software com sucesso. Os principais recursos de acessibilidade neste produto permitem que os usuários desempenhem as seguintes funções:

- Utilizar tecnologias de assistência, como softwares de leitor de tela e sintetizadores digitais de voz, para ouvir o conteúdo exibido na tela. Consulte a documentação do produto de tecnologia de assistência para obter detalhes sobre como utilizar essas tecnologias com este produto.
- Operar recursos específicos ou equivalentes utilizando apenas o teclado.
- Ampliar o conteúdo exibido na tela.

Além disso, a documentação deste produto foi modificada para incluir recursos de assistência à acessibilidade:

- Toda a documentação está disponível nos formatos HTML e PDF conversível para fornecer aos usuários a melhor oportunidade de aplicar softwares de leitor de tela.
- Todas as imagens na documentação são fornecidas com texto alternativo para que os usuários com deficiência visual possam compreender o conteúdo dessas imagens.

Navegando pela Interface Utilizando o Teclado

O produto utiliza o atalho padrão e as teclas de atalho que são documentados pelo sistema operacional. Consulte a documentação fornecida pelo seu sistema operacional para obter informações adicionais.

Ampliando o que É Exibido na Tela

Você pode ampliar as informações nas janelas do produto utilizando os recursos fornecidos pelos sistemas operacionais nos quais o produto é executado. Por exemplo, em um ambiente Microsoft Windows, você pode diminuir a resolução da tela para ampliar os tamanhos das fontes do texto na tela. Consulte a documentação fornecida pelo seu sistema operacional para obter informações adicionais.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 1616
3698
Doc.

10075

Apêndice E. Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte um representante IBM local, para obter informações sobre os produtos e serviços atualmente disponíveis em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138/146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para dúvidas relacionas a informações de DBCS (byte duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie as dúvidas, por escrito, para:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local. A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO-VIOLAÇÃO, MERCADO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias explícitas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. Alterações são periodicamente realizadas nas informações aqui constidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites não-IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites. Os materiais contidos nesses Web sites não fazem parte deste produto IBM e seu uso é de responsabilidade do Cliente.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1617
3698
Doc.

A IBM pode utilizar ou distribuir as informações fornecidas, da forma que julgar apropriada sem que incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que pretendam obter mais informações com o objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com a:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138/146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, dependendo dos termos e condições apropriadas, incluindo, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito nestas informações e todo o material licenciado disponível para o mesmo são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença do Programa Internacional IBM ou qualquer acordo equivalente.

As informações relativas a produtos não-IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não efetuou testes nestes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade ou qualquer outro requisito relacionado a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Estas informações contêm exemplos de dados e relatórios utilizados em operações diárias de negócios. Para ilustrá-las ao máximo possível, os exemplos incluem nomes de pessoas, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança a esses nomes e endereços utilizados por uma empresa comercial real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX	Magstar
Database 2	MQSeries
DB2	NetView
DB2 Universal Database	Redbooks
Enterprise Storage Server	RISC System/6000
ESCON	RS/6000
IBM	Tivoli
IBMLink	Tivoli Enterprise Console

Lotus, Lotus Notes e Domino são marcas ou marcas registradas da International Business Machines Corporation e da Lotus Development Corporation nos Estados Unidos e/ou em outros países.

Intel e Pentium são marcas ou marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

10073
A-

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada da Open Group nos Estados Unidos e/ou em outros países.

Java e todas as marcas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc., nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviços de terceiros.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1618
Doc. 3698

Glossário

Os termos neste glossário são definidos como pertencentes à biblioteca do IBM Tivoli Storage Area Network Manager. Se você não encontrar o termo necessário, consulte o IBM Software Glossary neste Web site: http://www.ibm.com/ibm/terminology/.

A

agente. Uma entidade que representa um ou mais objetos gerenciados (a) pela emissão de notificações referentes aos objetos e (b) pelo manuseio de solicitações de gerenciadores para operações de gerenciamento para modificar ou consultar os objetos. Consulte também *agente do IBM Tivoli Storage Area Network Manager*.

agente do IBM Tivoli Storage Area Network Manager. O software em um host gerenciado que executa funções locais, como monitoração do sistema de arquivos e discovery em banda. As funções são executadas em coordenação com o gerenciador.

C

coleta de dados. Consulte *discovery*.

console remoto. Um console do IBM Tivoli Storage Area Network Manager que é instalado em uma máquina diferente daquela em que o gerenciador está instalado. Um console remoto permite acessar o IBM Tivoli Storage Area Network Manager de qualquer localização.

D

discovery. O processo de localização de recursos dentro de uma empresa, incluindo a localização do novo local de recursos monitorados que foram movidos. No IBM Tivoli Storage Area Network Manager, o processo detecta recursos de armazenamento lógico e físico no ambiente de armazenamento e suas interconexões (também chamada de topologia). O IBM Tivoli Storage Area Network Manager também coleta atributos de recursos de armazenamento, tais como dados vitais do produto e medidas de capacidade e utilização. Discovery inclui a detecção de alterações na topologia da rede, tal como nós novos e excluídos ou interfaces novas e excluídas. Consulte também *intervalo de discovery*.

discovery em banda. O processo de descobrir informações sobre a SAN, incluindo dados de topologia e atributos, por meio de caminhos de dados do Canal de Fibras. Compare com *discovery fora da banda*.

discovery fora da banda. O processo de descobrir informações sobre a SAN, incluindo dados de topologia e dispositivos, sem utilizar os caminhos de dados do Canal de Fibras. Um mecanismo comum para discovery fora da banda é o uso de consultas MIB do SNMP, que são chamadas sobre uma rede TCP/IP. Compare com *discovery em banda*.

E

evento. No ambiente Tivoli, qualquer alteração significativa no estado de um recurso do sistema, recurso da rede ou aplicativo de rede. Um evento pode ser gerado para um problema, para a resolução de um problema ou para a conclusão de uma tarefa com êxito. Exemplos de eventos são: o início e a parada normais de um processo, a finalização anormal de um processo ou a falha de um servidor.

G

gerenciador. O componente do IBM Tivoli Storage Area Network Manager que é instalado em um host e fornece controle centralizado do produto. O gerenciador reúne dados de agentes SNMP e agentes em hosts gerenciados e fornece exibições gráficas de SANs. O gerenciador também pode transferir eventos para o Tivoli Enterprise Console ou um console do SNMP.

GUID (identificador globalmente exclusivo). Um código de 16 bytes que identifica uma interface para um objeto em todos os computadores e redes. O identificador é exclusivo porque contém uma data e hora e um código com base no endereço da rede que é conectado à placa da interface da LAN do computador host.

H

host. Um computador que é conectado a uma rede (como a Internet ou uma SAN) e fornece um ponto de acesso a essa rede. Além disso, dependendo do ambiente, o host pode fornecer controle centralizado da rede. O host pode ser um cliente, um servidor, um cliente e um servidor, um gerenciador ou um host gerenciado.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1619
Doc. 3698

host gerenciado. Um host que é gerenciado pelo IBM Tivoli Storage Area Network Manager. O host tem um agente do IBM Tivoli Storage Area Network Manager instalado e ativo nele. Os hosts gerenciados são utilizados para discovery em banda da SAN e para gerenciamento do sistema de arquivos.

I

intervalo de discovery. A freqüência na qual as informações de topologia e atributos são reunidas pelos agentes do IBM Tivoli Storage Area Network Manager e enviadas ao gerenciador. O intervalo de discovery é definido por um planejamento para que ocorra periodicamente ou em períodos específicos. Discovery também pode ocorrer em outros momentos, como quando disparada por um evento a partir da opção SAN.

L

LUN. Consulte *número da unidade lógica.*

N

nome da comunidade. A parte de uma mensagem do SNMP que representa um nome parecido com uma senha e que é utilizada para autenticar a mensagem do SNMP.

número da unidade lógica (LUN). Um identificador utilizado em um barramento SCSI para diferenciar entre dispositivos (unidades lógicas) com o mesmo ID do SCSI.

T

topologia. A disposição física e lógica de dispositivos em uma rede de área de armazenamento (SAN). A topologia pode ser exibida graficamente, mostrando os dispositivos e suas interconexões.

Índice Remissivo

A

acessibilidade 225
agentes
  AIX
    atualizando 151
    desinstalando 185
    início 93
    instalando 92
    instalando o Pacote de Idiomas 164
    parando 93
    requisitos para 12
  configurando 112
  desinstalando o Pacote de Idiomas 165
  função 1
  instalação automática 193
  Linux
    desinstalando 186
    início 93
    instalando 93
    instalando o Pacote de Idiomas 164
    parando 93
    requisitos para 13
  requisitos de armazenamento 10
  Solaris
    atualizando 151
    desinstalando 185
    início 92
    instalando 92
    instalando o Pacote de Idiomas 164
    parando 92
    requisitos para 13
  verificando arquivos de log 93
  Windows
    atualizando 146
    desinstalando 182
    início 92
    instalando 83
    instalando o Pacote de Idiomas 163
    parando 92
    requisitos para 12
ambiente da SAN 14
arquivo baroc
  como importar 116
  definição de 118
arquivo HOSTS
  alterando no Windows 22
  modificando 206
arquivos de log
  gerenciando logs de transação de DB2 202
  para gerenciador AIX 82
  para gerenciador Windows 77
  para hosts gerenciados 93
  para o console 105
  verificando 93
arquivos MIB
  ativando para o gerenciamento FC 213
  configurando 113
  para iSCSI 118
atualizando
  agente AIX 151
  agente Solaris 151
  agentes do Windows 146
  console remoto 139
  gerenciador Windows 129

B

Banco de dados MIB
  coletando informações para 2

C

comutador Brocade
  ativando a MIB de gerenciamento FC 213
configurando
  agentes 112
  dispositivos 108
  EDFI 123
  iSCSI 118
  o banco de dados DB2 201
  para enviar eventos 113
  para eventos do SNMP 113
  SAN sem hosts gerenciados 127
  Tivoli Enterprise Console 116
  traps do SNMP 8
  traps SNMP para o console de gerenciamento SNMP 111
  traps SNMP para o console Tivoli NetView 109
  traps SNMP para o Tivoli Storage Area Network Manager 110
conjuntos de regras
  carregando 123
  selecionando 126
considerações sobre compatibilidade 13
console de gerenciamento SNMP
  configurando para 111
Console do Tivoli NetView
  eventos suportados 2
console remoto
  ativando aplicativos a partir do 209
  atualizando 139
  desinstalando o Pacote de Idiomas 165
  iniciando no Windows 104
  instalação automática 195
  instalando 95
  instalando o Pacote de Idiomas no Windows 163
  números de porta 36
  parando no Windows 104
  removendo a instalação 178
console remoto *(continuação)*
  requisitos de armazenamento 10
  requisitos para 12
  verificando arquivos de log 105
contato por e-mail x

D

daemon do NetView
  início 210
  parando 210
  verificando 209, 210
DB2
  AIX
    desinstalando 187
    fazendo upgrade para o FixPak 8 46
    instalando 39
  configurando o banco de dados 201
  criando o servidor de administração no AIX 47
  criando uma instância do banco de dados no AIX 47
  fazendo upgrade de drivers JDBC no Windows 29
  gerenciando os logs de transação 202
  verificando no Windows 203
  Windows
    desinstalando 186
    fazendo upgrade para o FixPak 8 28
    instalando 22
descoberta
  definições padrões 3
  descoberta completa 3
  função 2
  iSCSI 7
descoberta fora da banda
  descrição de 211
  função 2
  informações reunidas 211
descoberta iSCSI
  arquivos MIB 118
  configurando 118
  início 121
  parando 122
  visão geral 5
descoberta na banda
  descrição de 211
  função 2
  informações reunidas 211
desinstalando
  pacote GUID Tivoli 177

E

EDFI
  carregando um conjunto de regras 123
  configurando 123

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - 233
CPMI - CORREIOS
Fls. Nº 1620
3698
Doc.

EDFI *(continuação)*
eventos 126
início 124
OIDs 127
parando 125
selecionando um conjunto de regras 126
visão geral 4
endereços IP estáticos
verificando no AIX 37
verificando no Windows 207
eventos
atributos 213
classes 213
como utilizado 210
configurando o IBM Tivoli Storage Area Network Manager para 113
configurando o Tivoli Enterprise Console para 116
controle 107
filtrando 107
IBM Tivoli Storage Area Network Manager 118
relatório da EDFI 126
Tivoli Enterprise Console 2
exceções
SNMP 2
exibição centrada no dispositivo 4
exibição centrada no host 4

G

gerenciador
AIX
desinstalando 177
desinstalando o Pacote de Idiomas 165
início 82
instalando 79
instalando o Pacote de Idiomas 162
números de portas para 35
parando 82
preparação para 35
visão geral das etapas 16
função 1
instalação automática 189
requisitos de armazenamento 10
requisitos para AIX 11
requisitos para Windows 10
Windows
atualizando 129
desinstalando o Pacote de Idiomas 165
início 76
instalando 59
instalando o Pacote de Idiomas 153
números de portas para 19
parando 76
preparação para 19
removendo a instalação 171
visão geral das etapas 16
gerenciando redes
visão geral 2

H

hosts gerenciados
AIX
desinstalando o agente 185
fazendo upgrade do agente 151
instalando o agente 92
instalando o Pacote de Idiomas 164
requisitos para 12
função 1
Linux
desinstalando o agente 186
instalando o agente 93
instalando o Pacote de Idiomas 164
requisitos para 13
números de portas com o gerenciador do AIX 36
números de portas com o gerenciador do Windows 21
removendo a instalação 182
Solaris
desinstalando o agente 185
fazendo upgrade do agente 151
instalando o agente 92
instalando o Pacote de Idiomas 164
requisitos para 13
Windows
desinstalando o agente 182
fazendo upgrade do agente 146
instalando o agente 83
instalando o Pacote de Idiomas 163
requisitos para 12

I

IDs do usuário
para gerenciador AIX 79
para gerenciador Windows 59
instalação automática
desinstalando o console remoto 198
desinstalando o gerenciador 198
desinstalando os agentes 198
para agentes 193
para console remoto 195
para o gerenciador 189
removendo a instalação 198
instalando
agentes em hosts 83
console remoto 95
DB2 no AIX 39
DB2 no Windows 22
gerenciador AIX
preparação para 35
procedimento para 79
visão geral das etapas 16
gerenciador Windows
preparação para 19
procedimento para 59
visão geral das etapas 16
Pacote de Idiomas
no console remoto 163
no gerenciador do AIX 162
no gerenciador Windows 153
instalando *(continuação)*
Pacote de Idiomas *(continuação)*
no host gerenciado do AIX 164
no host gerenciado do Linux 164
no host gerenciado do Solaris 164
no host gerenciado do Windows 163
visão geral 14
visão geral das etapas 14

L

lançando
aplicativos a partir do console remoto 209
logs de transação
gerenciando para DB2 202

M

manuais
feedback x

N

nome da comunidade
alterando 208
verificando 32
nomes de host completos
para AIX 205
para Linux 206
para Solaris 206
para Windows 22, 204, 206
nomes de hosts
abreviados 22, 206
completos 22, 206
longos 22, 206
verificando completos no AIX 37
verificando completos no Windows 21
números de porta
inserindo para o console remoto 99, 141
inserindo para o gerenciador do AIX 81
inserindo para o gerenciador do Windows 67
para console remoto 20, 36
para gerenciador AIX 35
para gerenciador Windows 19
para hosts gerenciados com o gerenciador do AIX 36
para hosts gerenciados com o gerenciador do Windows 21

O

OIDs
para EDFI 127

P

Pacote de Idiomas
desinstalando
agentes 165

10.068
A.

Pacote de Idiomas *(continuação)*
desinstalando *(continuação)*
no console remoto 165
no gerenciador do AIX 165
no gerenciador Windows 165
instalando
agente AIX 164
agente Linux 164
agente Solaris 164
agente Windows 163
console remoto 163
no gerenciador do AIX 162
no gerenciador Windows 153
pacote GUID Tivoli
diretórios 171
quando instalado 171
removendo a instalação 177
planejando a instalação 9
publicações
feedback x
publicações on-line viii

R

redes
gerenciando 2
removendo a instalação
agente AIX 185
agente Linux 186
agente Solaris 185
agente Windows 182
console remoto 178
DB2 no AIX 187
DB2 no Windows 186
gerenciador AIX 177
gerenciador Windows 171
Pacote de Idiomas
agentes 165
console remoto 165
no gerenciador do AIX 165
no gerenciador Windows 165
utilizando a desinstalação silenciosa 198
requisitos de armazenamento
para o Tivoli Storage Area Network Manager 10
requisitos de hardware
para agente do AIX 12
para agente do Linux 13
para console remoto 12
para gerenciador AIX 11
para gerenciador Windows 10
para o agente do Solaris 13
para o agente do Windows 12
para o Tivoli Storage Area Network Manager 10
requisitos de software
para agente do AIX 12
para agente do Linux 13
para console remoto 12
para gerenciador AIX 11
para gerenciador Windows 10
para o agente do Solaris 13
para o agente do Windows 12
para o Tivoli Storage Area Network Manager 10
requisitos do sistema
para o Tivoli Storage Area Network Manager 10

S

Serviço SNMP, instalando no Windows 29
servidor DB2
iniciando no Windows 204
parando no Windows 204
SNMP
alterando o nome da comunidade 208
definindo o nome da comunidade 110
gerando eventos 4
verificando o nome da comunidade 32
solicitando publicações ix
solução de problemas
problemas do Tivoli NetView 221
problemas do Tivoli Storage Area Network Manager 221
Suporte ao Cliente x
Suporte ao Cliente IBM x

T

Tivoli Enterprise Console
configurando o IBM Tivoli Storage Area Network Manager para 113
configurando para eventos 116
evento para a EDFI 126
eventos 213
eventos suportados 2
visão geral 116
Tivoli NetView
como configurar transferência de traps 109
criando entradas de trap 113
detectando problemas 221
dicas sobre como executar 209
topologia
descoberta 2
exibir 4
traps do SNMP
como utilizado 210
configurando 8, 109
configurando o IBM Tivoli Storage Area Network Manager para 113
configurando para o console de gerenciamento SNMP 111
configurando para o console Tivoli NetView 109
configurando para o Tivoli Storage Area Network Manager 110
enviando ao Tivoli Enterprise Console 116
suporte para 2

V

variável de ambiente EXTSHM 57

RQS nº 03/2005
CPMI - CORREIOS
Fls. Nº 1621
3698
Doc.