Doc.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – MANUAL VOLUME 8

2003
PASTA 36

ANEXO SWITCH TIPO 03
PARTE 10/A

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

Connectrix B Series systems have been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Contents

Preface

The EMC Connectrix B Series Diagnostic and System Error Message Reference Manual provides information on the diagnostic and system error messages that you may encounter during installation and operation of the DS-16B2, DS-32B2 and ED-12000B.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch and Enterprise Director. For the most up-to-date information on product features, see your product release notes.

If a feature in the DS-16B2, DS-32B2, or ED-12000B does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

Anyone involved in the installation, configuration, or management of the DS-16B2, DS-32B2, and ED-12000B.

Organization

Here is an overview of where information is located in this manual.

- Chapter 1, *System Error Message Formats*, contains general information about Fabric OS system error messages as well as information about viewing, reading, and understanding Fabric OS diagnostic command formats.
- Chapter 2, *v3.0 System Error Messages*, identifies, explains, and provides suggested recovery actions for Fabric OS version 3.0 system error messages.

- Chapter 3, *v4.0 System Error Messages*, identifies, explains, and provides suggested recovery actions for Fabric OS version 4.0 system error messages.
- Chapter 4, *General Diagnostic Error Message Information*, provides background information about diagnostic commands.
- Chapter 5, *Diagnostic Error Message Formats*, provides general information on diagnostic error messages.
- Chapter 6, *v3.0 Diagnostic Error Messages by Error Number*, identifies and provides detailed instructions and suggested recovery actions for diagnostic error messages related to Fabric OS version 3.0.
- Chapter 7, *v4.0 Diagnostic Error Messages by Error Number*, identifies and provides detailed instructions and suggested recovery actions for diagnostic error messages related to Fabric OS version 4.0.
- Appendix A, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix ED-12000B.
- The *Glossary* defines terminology used in this manual.

Related Documentation

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*

- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Manual

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this manual:

Palatino, bold	◆ Dialog box, button, icon, and menu items in text ◆ Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	◆ User entry. For example: **`symmpoll -p`** ◆ Options in command line syntax
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.emc.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.emc.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to `techpub_comments@emc.com` with your opinions of this manual.

1

Introduction to System Error Messages

This chapter provides an introduction to system error messages. It contains the following information:

Overview

This book supports Fabric OS version 4.1 and contains Diagnostic and System Error Messages with recommended actions. For ease of use, error messages are organized alphabetically first by module then by individual message.

Typically, each module contains multiple error messages and each error message contains message text, message explanation or probable cause, recommended action and severity level. There can be more than one cause and more than one recommended course of action for any given message. This document discusses the most probable cause and typical action recommended.

Error Message Severity Levels

There are 5 levels of severity messages ranging from 0 = Panic to 4= Information. In general, the definitions are broad-ranging and are to be used as general guidelines for troubleshooting. For all cases, it is advised to look at each specific error log description thoroughly before taking action. If you have any questions, collect the applicable data then contact EMC Customer Support Center for further clarification. Error messages have the following severity levels:

0 = Panic	Panic level messages indicate a specific software subsystem has detected a fatal/irrecoverable error condition. For example: memory allocation failures, system call failures, software detection of misbehaving ASIC or hardware subsystems. Such errors indicate either partial or complete failure of a subsystem. A panic may frequently result in a reboot of a single-processor switch or a failover of an ED-12000B operating in a fully redundant state.
1 = Critical	Critical level messages indicate serious problems detected by the software which will eventually cause a partial or complete failure of a subsystem. For example: a power supply failure or sensor failure can cause a critical level error message to report. Some of the critical errors may overlap in severity with the Panic level messages.
2 = Error	Error level messages indicate error conditions that may not be considered fatal. These messages are considered to be less severe than Panic or Critical error messages. For example, error level messages may indicate timeouts seen on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = Warning	Warning messages are less severe than error messages. These messages may indicate temporary failures detected by a software module. An example may include a detection of a parameter under monitoring that exceeded a specific threshold value.
4 = Info	Information messages are purely informational that record important events in the system. For example, disabling a port or clearing the switch error log.

Overview of the System Logs

This section provides information on the System Logs in the system, the types of messages saved, and how to view the information in the log files.

The contents of the Port Logs and setting up syslogd are discussed in the *Fabric OS Procedures Guide*. The contents of the Panic Trace logs are intended for support use only.

System Error Log

The Fabric OS maintains an internal System Error Log of all diagnostic and system error messages. The internal log buffers are limited in size; when the internal buffers are full, new messages overwrite old messages.

Features of the System Error Log:

- Each switch has a System Error Log, by default messages of Panic and Critical level are saved to flash (using the Persistent Error Log feature see *Persistent Error Log* on page 1-5) and all other messages are volatile. Messages not saved to flash are lost over power cycles and reboots.
- The System Error Log can save a maximum of 1536 messages in RAM, that is, a total of 256 messages for each error message level (Panic, Critical, Error, Warning, Info, and Debug).
- The System Error Log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are over-written by new entries.
- When the switch is rebooted the System Error Log messages saved in RAM are lost. Those messages in the System Error Log not saved to the Persistent System Error Log are NOT preserved across power cycles and system reboots.
- By default the `errdump` and `errorshow` commands display all the system error messages, that is, volatile error messages (saved in memory) and persistent error messages (saved in flash) together. Operands for these commands enable you to display either messages in (volatile) System Error Log, or messages saved to the Persistent Error Log.

Persistent Error Log

The Persistent Error Log feature enables messages to be saved across power cycles and reboots. It also prevents messages of lesser severity from over-writing messages of greater severity. For example, *Warning* messages cannot over write *Error*, *Critical*, or *Panic* messages.

Features of the Persistent Error Log:

- Messages in the Persistent Error Log are preserved across power cycles and system reboots.
- (ED-12000B specific) The Persistent Error Log is saved to the current active CP and is not carried over to the new active CP in the event of a failover. Each CP on an ED-12000B has a unique Persistent Error Log, depending on the messages saved when that CP was the active.
- The Persistent Error Log has a default capacity to store 1024 error log entries.
- The Persistent Error Log can be resized (between 1024 and 2048 entries) at run time without having to reboot the switch or the system. Use the **errnvlogsizeset** to set the size of the Persistent Error Log, and the **errnvlogsizeshow** command to view the current configuration.
- The Persistent Error Log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are over-written by new entries.
- All error messages of levels Panic and Critical are by default saved in the Persistent Error Log as they are logged. This guarantees that critical or panic level messages are not lost in the event of unexpected system reboot or fail-over.
- The message level saved to the Persistent Error Log can be modified. Use the **errsavelvlset** to set the threshold level of messages saved to the Persistent Error Log, and the **errsavelvlshow** command to view the current threshold configuration.
- Use the **errclear** -p command to clear the Persistent Error Log.

Only the Persistent Error Log can be resized. The System Error Log cannot be resized.

Syslogd Daemon

Syslogd is a process that runs on UNIX or LINUX systems that reads and logs messages to the system console, log files, other machines and users as specified by its configuration file. Refer to the manual pages and related documentation for your particular UNIX host system for more information on the syslogd process and its capabilities.

The Fabric OS can be configured to use a UNIX style syslog daemon (syslogd) process to read system events and error messages and forward these messages to users and/or write the events to log files on a remote UNIX host system.

The Connectrix switch can be configured to send error log messages to a UNIX host system that supports syslogd. This host system can be configured to receive error/event messages from the switch and store them in files on the computer hard drive. This enables the storage of switch error log messages on a host system and overcomes the size limitations of the internal log buffers on the Connectrix switch.

The host system can be running UNIX, Linux or any other operating system as long as it supports standard syslogd functionality. The ED-12000B or DS-32B2 itself does not assume any particular operating system to be running on the host system. The only requirement is that the host system must support standard syslogd to receive error log messages from the ED-12000B or DS-32B2.

For information on configuring the syslogd functionality, refer to the *Fabric OS Procedures Guide*.

Port Logs

The Fabric OS maintains an internal Port log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular log files, which can save up to 8000 entries per logical switch. Once the log is full, the newest log entries over-write the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some deviceA-to-deviceB, and control information. Port logs are not persistent and are lost over power-cycles and reboots.

Use the **portlogshow** command to display the Port logs for a particular port.

Use the **portlogeventsshow** command to display the specific events reported for each port.

Refer to the *Fabric OS Procedures Guide* for information on interpreting the **portlogdump** command.

The port log functionality is completely separate from the System Error Log functionality. Port logs are typically used to troubleshoot connection of devices.

Panic Trace Log

The Panic Trace Log is created by a system watchdog process when problems are encountered in the Fabric OS kernel. These files build up in the kernel partition (typically because of failovers) and should be periodically deleted or downloaded using the **savecore** command. In case of a kernel panic, trace files are created which can be viewed with the **pdshow** command.

System Watchdog Process

The Software Watchdog Process (SWD) is responsible to monitor applications critical to the function of a health switch. The SWD holds a list of critical daemons and it expects them to ping periodically at a predetermined amount of time. This time varies per application.

In the event that an application failed to ping the SWD within the given amount of time or if the application terminates unexpectedly, then the SWD activates and dumps information to the Panic Trace Log that enables Support to diagnose the unexpected error.

Use the **pdshow** command to view these files or the **savecore** command to FTP them to a host workstation.

The Panic Trace Log files are intended for support purposes only, and are not intended for end user use.

System Console

The System Console displays messages through the serial port. If you telnet into the ethernet port, you will not receive console messages. The System Console displays both System Error Messages and Panic Trace messages. These messages are only mirrored to the system console, and are always saved in one of the system logs.

View or Configure System Logs

The following commands are used to view or configure the error logs:

Table 1-1 **Commands Used to View or Configure the System Logs**

Command	Description
agtcfgdefault	Reset the SNMP recipients to default values.
agtcfgset	Configure the SNMP recipients.
agtcfgshow	Display the current configuration of the SNMP recipients.
errclear	Clear the error log.
errdump	Display the entire error log with no page breaks.
errnvlogsizeset	Set the size of the persistent error log.
errnvlogsizeshow	Display the size of the persistent error log.
errsavelvlset	Set the level threshold of messages saved to the error log.
errsavelvlshow	Show the level threshold of messages saved to the error log.
errshow	Display the entire error log with page breaks.
memshow	Display the current memory usage of the switch.
pdshow	Display the contents of the Panic Trace log.
porterrshow	Display the port error summary.
portflagsshow	Display the port status bitmaps for all ports in a switch
portlogclear	Clear the port log. If the port log is disabled, this commands enables it.
portlogdisable	Disable the port log facility.
portlogdump	Display the port log without page breaks.
portlogdumpport	Display the port log of specified port, without page breaks.
portlogeventshow	Displays which port log events are currently being reported.
portloginshow	Display port logins.
portlogpdisc	Set or clear the debug pdisc_flag.

Table 1-1 Commands Used to View or Configure the System Logs (continued)

Command	Description
portlogreset	Enable the port log facility.
portlogresize	Resize the port log to the specified number of entries.
portlogshow	Display the portlog with page breaks.
portlogshowport	Display the port log of specified port, with page breaks.
portlogtypedisable	Disable an event from reporting to the portlog. Portlog events are described by the **portlogeventshow** command.
portlogtypeenable	Enable an event to report to the portlog. Portlog events are described by the **portlogeventshow** command.
savecore	Save or remove core files created by the kernel.
setdbg	Set the level of debug messages reported by a particular module.
seterrlvl	Set the level of errors reported by a particular module.
setverbose	Set the verbose level of a particular module within the Fabric OS.
supportshow	Executes a list of diagnostic and error display commands. This output is used by support to diagnose and correct problems with the switch. The output from this command can be very long.
syslogdipadd	Add an IP address as a recipient of event/error messages.
syslogdipremove	Remove an IP address as a recipient of event/error messages.
syslogdipshow	View the currently configured IP addresses who are recipients of event/error messages.

Reading a System Error Message

This section provides information about reading System Error Messages. System Error Messages are typically generated by the various modules in the Fabric OS. They are dumped in the System Error Log and depending on severity may be saved to memory or flash.

Viewing System Error Messages from Web Tools

To view the System Error Log for a switch from Web Tools:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Select the Switch Events button from the Switch View.
4. A Switch Events Report appears.
5. View the switch events and messages.

Displaying the Error Log Without Page Breaks

To display the switch error log all at once:

1. Log in to the switch as the admin user.
2. Enter the **errdump** command at the command line.

Example

```
switch:admin> errdump

Error 04
--------
0x576 (fabos): Mar 25 08:26:44 (1)
Switch: 1, Info TRACK-LOGIN, 4, Successful login

Error 03
--------
0x576 (fabos): Mar 24 16:01:44 (12)
Switch: 1, Info TRACK-CONFIG_CHANGE, 4, Config file
   change from task:ZNIPC

Error 02
--------
0x2f0 (fabos): Mar 24 15:07:01
Switch: 1, Warning FW-STATUS_SWITCH, 3, Switch status
   changed from HEALTHY/OK to
 Marginal/Warning

Error 01
--------
```

```
0x271 (fabos): Mar 24 15:04:06
Switch: 1, Info EM-BOOT, 4, Restart reason: Failover

switch:admin>
```

Displaying the Error Log With Page Breaks

To display the error log:

1. Log in to the switch as the admin user.
2. At the command line enter the `errshow` command.

```
switch:admin> errshow

Error 497
--------
0x4a5 (fabos): Oct 03 04:40:14
Switch: 0, Info TRACK-LOGIN, 4, Successful login

Type <CR> to continue, Q<CR> to stop: q
```

Clearing the Switch Error Log

To clear the error log for a particular switch instance:

1. Log in to the switch as the admin user.
2. Enter the `errclear -p` command to clear only the persistent errors. The error log in RAM is not cleared.

   or

   Enter the `errclear` command (with no operands) to clear the RAM memory, and remove persistent messages from the default `errshow` display.

   If no operand is specified, this command changes the way the error log appears in subsequent sessions. By default, the `errshow` command displays both the persistent and active log sessions. However, in future sessions you would have to use the `errshow -p` command to view persistent error messages.

The following example shows how to clear the persistent error log on the Active CP.

```
switch:admin> errclear -p
switch:admin>
```

Setting the Error Save Level of a Switch

To control types of messages that are saved in the persistent error log:

1. Log in to the switch as the admin user.
2. At the command line enter the `errsavelvlset` command.

The following example shows how to enable saving of Warning, Error, Critical and Panic messages in the persistent error log.

```
switch:admin> errsavelvlset 3
switch:admin>
```

By default, all messages of type Panic and Critical are saved in the persistent log.

Displaying the Current Error Save Level Setting of a Switch

To find out the current value of the persistent error log save level for a given switch instance:

1. Log in to the switch as the admin user.
2. Enter the **errsavelvlshow** command at the command line.

The following example shows how to display current error log save level.

```
switch:admin> errsavelvlshow

 Current message save level is = 3

switch:admin>
```

The following example shows how to display current error log save level on the Standby CP for switch 0.The value -s is added to save the Standby CP.

```
switch:admin> errsavelvlshow -s 0

 Current message save level is = 3

switch:admin>
```

Resizing the Persistent Error Log

To resize the persistent error log of a switch to a new size specified by the operand `number_of_entries`:

1. Log in to the switch as the admin user.
2. At the command line enter the `errnvlogsizeset` command.

The following example shows how to resize the persistent error log to 1500 entries.

```
switch:admin> errnvlogsizeset 1500

Persistent error log is  resized to store 1500 entries

switch:admin>
```

Example Error Log Message

The following example shows a sample message from the error log.

```
Error 1001
--------
0x253 (fabos): Nov 03 14:11:53
Switch: 1, Error EM-CP_ERR, 2, CP in slot 5 set to
   faulty because of CP ERROR
```

The fields in the error message are described in Table 1-2.

Table 1-2 Error Message Field Description

Example	Variable Name	Description
`Error 1001`	Error Log Buffer Number	Displays a rotating number that describes the position the message holds in your buffer. This number is not permanently affiliated with the error itself and should *not* be used when contacting Tech Support.
`Nov 03 14:11:53`	Date and Time	Displays the date and time the error message occurred.
`Switch: 1`	Switch: <number>	Displays the logical switch that was affected (will be 0 or 1).
`Error`	Severity Level	Displays the severity of the message: Panic, Critical, Error, Warning, or Info.
`EM-CP_ERR`	Error Module - Error Code	Displays the module name that generated the error, and the code name for the error.
`2`	Severity Level	Displays the severity of the error in a numbered format. 0 = Panic 1 = Critical 2 = Error 3 = Warning 4 = Info 5 = Debug
`CP in slot 5 set to faulty because of CP ERROR`	Error Description	Displays error specific data, such as the error reason.

Responding to a System Error Message

This section provides information on responding to System Error messages.

Looking Up an Error Message

Error messages are arranged in this manual by module. To look up an error message, determine the module and the error code and compare this with the Table of Contents to determine the location of the information for that error message.

Information provided by this book:

- Message Text
- Firmware module that generated the error
- Module and Code name for the error
- Probable cause
- Appropriate response

Gather Information about the Problem

Common steps and questions to ask to help troubleshoot a System Error message:

1. Run supportshow and pdshow, save the output then provide to Technical Support for assistance in troubleshooting.
2. Can you document the sequence of events?
3. Did a Failover occur?
4. Was Security enabled?
5. Was POST enabled?
6. Are serial port (console) logs available?
7. Which CP was master?
8. What was the last change made?

Common Responses

Listed below are common responses to System Error messages:

- Run supportshow, and pdshow then provide a copy to technical support.
- Gather logs
- Watch for re-occurrence

- Re-install firmware
- Reboot machine
- Revert to previous firmware version
- Call support

2

AS_System Error Messages

This chapter contains the following section:

Introduction

Alias Server provides a multi-casting capability: a single frame can be delivered to multiple ports. The user defines a group of ports identified by the Alias ID, and delivers a frame to that group using the Alias ID, and the Alias Server daemon tracks the Alias ID.

AS-CTMALLOC

Message

```
<switch number> Error AS-CTMALLOC, 2, <variable> :
   ctMalloc for <number of bytes> bytes failed <variable>
```

Explanation Memory allocation failure. Fabric OS error.

Recommended Action Copy the name of the error (AS-CTMALLOC) and call EMC Customer Support .

Severity Error

3

Blade_System Error Messages

This chapter includes the following section:

Introduction

Blade error messages are a result of faulty hardware, transient out of memory conditions, ASIC errors, inconsistencies in the software state between a blade and the EM (Environment Monitor) module.

BLADE-FAULT

Message `<switch number> Critical BLADE-FAULT, 1, Faulting blade in slot <slot number>`

Explanation A problem was reported with the blade specified in *<slot number>*.

Action Try cycling power on the specified blade using **slotpoweroff** and **slotpoweron**. If the error recurs, contact EMC Customer Support Center.

Severity Critical

BLADE-INIT_FAIL

Message `<switch number> Critical BLADE-INIT_FAIL, 1, Init Failed: <reason string>, Slot: <slot number>`

Explanation The blade initiation failed for the specified *<slot number>*. The specified blade is faulted.

Action Additional blade fault messages will follow this error, to provide additional information. See specific error messages for recommended action.

Severity Critical

BLADE-OUT_OF_MEMORY

Message

```
<switch number> Critical BLADE-OUT_OF_MEMORY, 1,
   <function> : <failed function call>, out of memory
   condition
```

Explanation

The switch is low on memory and failed to allocate new memory for an Information Unit.

The <*function*> will be "minis_rx_tasklet".

The <*failed function call*> will be "iu_alloc failed". This function call is for memory allocation for information units.

Action

This usually signifies a transient memory shortage. A non-bladed switch will automatically reboot. For a bladed switch, the active CP card will automatically failover, and the standby CP will become the active CP. If the error message persists, contact EMC Customer Support Center.

Severity

Critical

BLADE-REG_FAULT

Message

```
<switch number> Critical BLADE-REG_FAULT, 1, ASIC driver
   detected Slot <slot number> port <port number> as
   faulty (reason: <reason>
```

Explanation

A blade regulation problem was reported on the specified <*slot number*>. The blade will be faulted.

Action

Resolve the specified <*reason*> as described in the error message. If the error persists, copy the error message and contact EMC Customer Support Center.

Severity

Critical

4

Bloom_System Error Messages

This chapter contains information on the following:

Introduction

Bloom is the name of the ASIC used as the building block for EMC's third generation hardware platforms.

BLOOM-AVAILABLE_BUF_OVERFLOW

Message `<switch number> Panic BLOOM-AVAILABLE_BUF_OVERFLOW, 0, S<slot number>, P<port number>(<blade port number>): quadpt <quad number> available buffer overflow: avail <available buffers>`

Explanation Buffer requested exceeds maximum available buffer number for the specified slot and port. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-BAD_ID

Message `<switch number> Warning BLOOM-BAD_ID, 3, S<slot number>, P<port number>(<blade port number>): IU in <message string> has bad ID (S_ID = <SID number>, D_ID = <DID number>)`

Explanation A bad source ID or destination ID was reported on the specified slot and port number.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Warning

BLOOM-BE_PORT_BUF_TO

Message `<switch number> Panic BLOOM-BE_PORT_BUF_TO, 0, S<slot number>, P<port number>(<blade port number>): no buffers for the backend port, bufs_rdy=<buffer number>`

Explanation No buffers are available for the backend port of the specified slot and port number. The specified slot will be disabled.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-BE_SYNC

Message `<switch number> Panic BLOOM-BE_SYNC, 0, S<slot number>, P<port number>(<blade port number>): Backend port disabled due to sync problem, lli_status= <lli status number>`

Explanation The backend port could not reach the sync state for the specified slot and blade port number. The specified blade port will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-BE_TRUNK

Message `<switch number> Panic BLOOM-BE_TRUNK, 0, S<slot number>, P<port number>(<blade port number>):Trunk group is down -- this blade is fault, lli_status=<LLI status number?>`

Explanation The trunk group is down for the specified slot and port. The specified slot will be faulted. The Low Level Interface (LLI) status provides additional error information.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-BISR_FAILED

Message `<switch number> Panic BLOOM-BISR_FAILED, 0, S<slot number>, P<port number>(<blade port number>):cmBisr failed. slot <number?> chip <chip number> fail <failure number> done <done number> mask <done mask>`

Explanation A failure of the Central Memory built-in-self-repair was reported for the specified slot and port. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-BUF_RECLAIMED

Message

```
<switch number> Info BLOOM-BUF_RECLAIMED, 4, <port number>
```

Explanation If the specified port was previously disabled because no buffer was available, the port is now enabled since some buffer has been made available in the same quad.

Action No action required.

Severity Info

BLOOM-CMEM_ERR

Message

```
<switch number> Warning BLOOM-CMEM_ERR, 3, S<slot
   number>, P<port number>(<blade port number>):cmem
   error, buf_error: <buffer error number>
```

Explanation A port Central Memory buffer error was reported for the specified slot and port.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support Customer Support may also ask for additional debug information from POST and systemtest.

Severity Warning

BLOOM-CMI_ERR

Message `<switch number> Warning BLOOM-CMI_ERR, 0, S<slot number>, P<port number>(<blade port number>):cmi error, err_status <CMI error number> (addr:<error status h/w address>), cmi_st <cmi status number>`

Explanation A CMI (Central Memory Interface) bus error was reported for the specified slot and port. The specified slot will be disabled.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-DISABLE_MINIS

Message `<switch number> Warning BLOOM-DISABLE_MINIS, 3, S<slot number>, P<port number>(<blade port number>):port fault reason = <reason number>, disable the mini-switch.`

Explanation A fault was reported for the specified port and slot while diagnostics was running. The miniswitch will be disabled for the specified slot and port number.

Action Run `portlogdisable` and `supportshow` to capture debug information from these commands then contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest. The error message details are used for debugging.

Severity Warning

BLOOM-EMB_PORT_BUF_TO

Message `<switch number> Panic BLOOM-EMB_PORT_BUF_TO, 0, S<slot number>, P<port number>(<blade port number>): no buffers for the embedded port <quad number>`

Explanation The embedded processor port could not get the requested buffer for the specified slot and port. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-EXCESSIVE_BUSY_MINI

Message `<switch number> Panic BLOOM-EXCESSIVE_BUSY_MINI, 0, S<slot number>, P<port number>(<blade port number>):quadpt <quad number> excessive busy_mini for ep: <embedded port buffer value>`

Explanation The mini buffer requested from the embedded processor port exceeds maximum available buffer number for the specified slot and port.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-EXCESSIVE_RCC_VC

Message `<switch number> Panic BLOOM-EXCESSIVE_RCC_VC, 0, S<slot number>, P<port number>(<blade port number>):excessive rcc_vc: current = <current RCC VC number>, default = <default RCC VC number>`

Explanation The Receive Credit Counter (RCC) credits for receiving frames has exceeded the default buffers granted on the specified virtual channel. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-FDET_BUFTAG

Message `<switch number> Panic BLOOM-FDET_BUFTAG, 0, S<slot number>, P<port number>: SOF <start of Frame/Buffer Tag> or EOF <end of Frame/Buffer Tag> buftag !=<Expected Buffer Tag`

Explanation A mismatched frame buffer number identifier (buffer tag) was received on the specified slot and port. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-FDET_ERR

Message `<switch number> Panic BLOOM-FDET_ERR, 0, S<slot number>, P<port number> (<blade port number>): fdet(<error message string>`

Explanation A hardware internal failure detection error was reported for the specified slot and port. The specified slot will be faulted.

Action Copy error message and call Customer Support .

Severity Panic

BLOOM-FDET_ERR_X

Message `<switch number> Panic BLOOM-FDET_ERR_X, 0, S<slot number>, P<port number>: fdet(<identification message string>`

Explanation This hardware internal failure detect supplemental message (see BLOOM-FDET_ERR) is used to trigger additional debugging data for internal manufacturing debugging.

Action Copy the identification message string and call Customer Support .

Severity Panic

BLOOM-INCONSISTENT

Message `<switch number> Panic BLOOM-INCONSISTENT, 0, inconsistent in <message string>`

Explanation Inconsistency reported in the bloom driver. One of the following inconsistent scenarios was reported:

- <List D trigger>
  Explanation: Unexpected filter LISTD frame received.
- <Mix ASIC revs>
  Explanation: Mixed BLOOM ASIC chip versions.
- *<Virtual pool usage>*
  Explanation: Mismatched between allocated and expected virtual memory locations.
- *<Missing sorted cam>*
  Explanation: Missing CAM entry from the sorted CAM table.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-INCONSISTENT_EXT

Message

```
<switch number> Panic BLOOM-INCONSISTENT_EXT, 0, S<slot
  number>, P<port number>(<blade port number>):
  inconsistent in <message>
```

Explanation

Inconsistency was reported in the bloom driver. The specific slot and port number is reported in this error, and the *<message>* provides additional information for troubleshooting. One of the following inconsistent scenarios was reported:

- <Process require list is empty2>
  Explanation: An unexpected processing required interrupt was reported for the specified slot and port. The specified port will be faulted.
- <BloompollLism odd_buf <buffer number>
  Explanation: An invalid buffer number was obtained for LISM frame transmission. The buffer allocation will be retried.
- <Bloomwrrxbdesc odd_buf <buffer number> to blm <address>
  Explanation: An invalid buffer number was obtained for frame transmission.
- <RX overflow/TX FIFO under/overflow. buf_err=<buffer error>
  Explanation: An unexpected central memory buffer error was reported for the specified slot and port.
- <Detect error port stuck INT_CMEM_ERR @ 2GPS>
  Explanation: An unexpected central memory buffer error was reported for the specified slot and 2G port.
- <Error: unknown CMEM error type <error type>
  Explanation: An unknown central memory error was reported for the specified slot and port.
- <No filter port>
  Explanation: No matching filter port was reported for the specified slot and port.
- <BloomBXOnline>
  Explanation: No user port was found in the miniswitch or was found on the specified slot and port.
- <RX Overflow on 1G =>CMEM Error buf_error=<buffer error>
  Explanation: An unexpected central memory error was reported for the specified slot and 1G port. The specified slot will be faulted.

- <LISM no nuffer>
  Explanation: No buffer available for sending LISM frame on the specified slot and port.
- <Sticky secondary Tx parity error>
  Explanation: A central memory error was reported and forced a TX parity error for the specified slot and port. The specified slot will be faulted.
- <Bad LoadBuf state <state>>
  Explanation: An unexpected state was reported while obtaining buffers for the specified slot and port.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information from these commands then contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-INVALID_LIST_TRIGGER

Message `<switch number> Panic BLOOM-INVALID_LIST_TRIGGER, 0, S<slot number>, P<port number>(<blade port number>): Unknown list triggered`

Explanation An unknown filter list interrupt was reported for the specified slot and port. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-LISTD_TRIGGER

Message `<switch number> Panic BLOOM-LISTD_TRIGGER, 0, S<slot number>, P<port number>(<blade port number>): List D triggered`

Explanation An unexpected filter list interrupt was reported for the specified slot and port. The specified slot will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-MALLOC

Message `<switch number> Panic BLOOM-MALLOC, 0, malloc failed in <message string>`

Explanation One of the following memory allocation failures was reported:

- *<bloomPortInstantiate>*
  Explanation: Failed initializing bloom port data structure
- *<filterQuadAlloc>*
  Explanation: Failed to allocate filter zone group data structure
- *<zone group buffer>*
  Explanation: Failed to allocate zone group data structure
- *<cam zone buffer>*
  Explanation: Failed to allocated cam zone buffer structure
- *<vital hardware>*
  Explanation: Failed to allocated memory for virtual pool structure
- *<real cam next>*
  Explanation: Failed to allocate memory for real cam next array structure
- *<real to virtual cam table>*
  Explanation: Failed to allocate memory for real to virtual translation array
- *<real zone group next>*
  Explanation: Failed to allocate memory for dedicated real zone group next index
- *<real to virtual>*
  Explanation: Failed to allocate memory for dedicated real to virtual translation structure
- *<Not enough memory for virtual>*
  Explanation: Not enough memory for virtual hardware function.
- *<bloomChipInstanitate>*
  Explanation: Failed initializing chip data structure.

Action Copy the error message string, run `memshow` and `supportshow` to capture debug information, then call Customer Support .

Severity Panic

BLOOM-MALLOC_EXT

Message `<switch number> Panic BLOOM-MALLOC_EXT, 0, S<slot number>, P<port number>(<blade port number>):: malloc failed in <message string>`

Explanation One of the following memory allocation failures was reported for the specified slot and port:

- *<bloomPortInstantiate>*
  Explanation: Failed initializing data structure in bloomPortInstantiate
- *<bloomFAN - 1>*
  Explanation: Failed to allocate Fabric Address Notification IU location 1
- *<bloomFAN - 2>*
  Explanation: Failed to allocate Fabric Address Notification IU location 2
- *<bloomWrRetTxBuffer>*
  Explanation: Failed to allocate IU in bloomWrRetTxBuffer()
- *<bloomBufAllocIU>*
  Explanation: Failed to allocated IU in bloomBufAllocIU()

Action Copy the error message string, run `memshow` and `supportshow` to capture debug information, then call Customer Support .

Severity Panic

BLOOM-MINI_BUFFER

Message

```
<switch number> Warning BLOOM-MINI_BUFFER, 3, <quad number>
```

Explanation Two or more bad hardware buffers are reported from the specified quad.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POSt and systemtest.

Severity Warning

BLOOM-NO_BUFFERS

Message

```
<switch number> Warning BLOOM-NO_BUFFERS, 3, S<slot
   number>, P<port number>(<blade port number>): port
   <port number> disabled due to lack of buffers
```

Explanation The specified slot and port were disabled due to lack of available buffers. This usually happens when one or more ports in the same quad are configured as long distance.

Action Disable one or more other ports in the same quad in order to enable the specified slot and port.

Severity Warning

BLOOM-NULL_PTR

Message `<switch number> Panic BLOOM-NULL_PTR, 0, NULL ptr in <message string>`

Explanation One of the following NULL pointer scenarios was reported:

- *<bloomPortAttach: p>*
  Explanation: NULL p pointer detected in bloomPortAttach()
- *<bloomPortAttach: qdpblm>*
  Explanation: NULL quad pointer detected in bloomPortAttach()
- *<bloomChipAttach: chblm>*
  Explanation: NULL chblm pointer detected in bloomChipAttach()
- *<bloomChipAttach: c>*
  Explanation: NULL virtual chip pointer detected in bloomChipAttach()
- *<bloomChipAttach>*
  Explanation: NULL memory map pointer detected in bloomChipAttach()

Action Copy the error message, run `supportshow` to capture debug information contact EMC Customer Support Center with information.

Severity Panic

BLOOM-NULL_PTR_EXT

Message `<switch number> Panic BLOOM-NULL_PTR_EXT, 0, S<slot number>, P<port number>(<blade port number>):: NULL ptr in <message string>`

Explanation One of the following NULL pointer scenarios was reported:

- <bloomPortInstantiate>
  Explanation: NULL pointer detected in bloomPortInstantiate()
- *<bloomPortInit>*
  Explanation: NULL pointer detected in bloomPortInit()
- *<bloomSendLinitFrame>*
  Explanation: NULL pointer detected in bloomSendLinitFrame()

Action Copy the error message, run `supportshow` to capture debug information contact EMC Customer Support Center with information.

Severity Panic

BLOOM-OVERRUN_INT_RCVD

Message `<switch number> Panic BLOOM-OVERRUN_INT_RCVD, 0, S<slot number>, P<port number>(<blade port number>):mem overrun, quad: <quad number>`

Explanation A central memory buffer could not be allocated for the specified slot and port. The specified slot and port will be faulted.

Action Run `portlogdisable` and `supportshow` (in order) to capture debug information and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-PORT_INIT_STUCK

Message

```
<switch number> Panic BLOOM-PORT_INIT_STUCK, 0, S<slot
   number>, P<port number>(<blade port number>):port init
   stuck in <messages string> loop <loop status> <TX from
   RX status> busy_buf[4] <busy buffer>
```

Explanation One of the following scenarios was busy transitioning to the next state on the specified slot and port.

- *<bloomLismCleanup: LIP received>*
  Explanation: Loop initialization frames could not be flushed after receiving LIP on the specified slot and port.
- *<bloomLismCleanup: become Master>*
  Explanation: Loop initialization frames could not be flushed after becoming loop master on the specified slot and port.
- *<bloomLismCleanup: Not Master>*
  Explanation: Loop initialization frames could not be flushed after the specified slot and port determined it was not the loop master.
- *<going to the OLD_PORT state>*
  Explanation: The specified slot and port could not transition to the OLD_PORT state.
- *<waiting for LPC OPEN state>*
  Explanation: The specified slot and port (loop port control) could not transition to the OPEN state
- *<entering OPEN_INIT ALPA>*
  Explanation: The specified slot and port could not transition to the OPEN_INIT_ALPA state.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-RAMINIT_TO

Message `<switch number> Critical BLOOM-RAMINIT_TO, 1, S<slot number>, P<port number>(<blade port number>):port <port number> failed to init RAM @ <offset>, busy status=<busy index>`

Explanation RAM initialization cannot be completed within the expected time for the specified slot and port number.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Critical

BLOOM-RAM_PAR_ERR

Message `<switch number> Panic BLOOM-RAM_PAR_ERR, 0, S<slot number>, P<port number>(<blade port number>): epil_status: <embedded port status> R2T: <RX to TX ram parity> TFR: <TX to RX ram parity> STATS: <statistics> SMI: <SMI> FLT: <filter> PHAN: <phantom> EFD: <failure detect>`

Explanation RAM parity error was reported for the specified slot and port. The specified slot will be faulted.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-SMI_STUCK_WR

Message `<switch number> Warning BLOOM-SMI_STUCK_RD, 3, S<slot number>, P<port number>(<blade port number>): read mini port <miniswitch port> stuck at SMI op=<memory control>(prev=<direction>)`

Explanation The specified slot and port was unable to write into central memory.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Warning

BLOOM-SPEED_TO

Message `<switch number> Info BLOOM-SPEED_TO, 0, S<slot number>, P<port number>(<blade port number>): Speed negotiation failed: Faulting port <port>`

Explanation The specified slot and port was unable to negotiate speed. The specified slot and port will be faulted and speed negotiation will be restarted.

Action If problem persists, replace cable, SFP or check device connected to the specified slot and port. If problem continues to persist, run `portlogdisable` and `supportshow` (in order) to capture debug information from these commands and contact EMC Customer Support Center.

Severity Info

BLOOM-STUCK_WAIT

Message

```
<switch number> Panic BLOOM-EXCESSIVE_BUSY_MINI, 0, <port number> <Loop
   status> <TX-from-RX status> busy <busy buffer value> <message string>
```

Explanation One of the following scenarios was busy transitioning to the next state on the specified slot and port.

- *<waiting for OPEN state>*
  Explanation: The specified port could not transition to the OPEN state.
- *<waiting for CLOSE state>*
  Explanation: The specified port could not transition to the CLOSE state
- *<init stuck at bloomLPC waiting for OPEN state>*
  Explanation: The specified port could not transition to the OPEN state when executing the LPC command.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-SUSPENDED_INT_RCVD

Message `<switch number> Panic BLOOM-SUSPENDED_INT_RCVD, 0, S<slot number>, P<port number>(<blade port number>):int suspended (status=<interrupt status>, mask=<interrupt mask>)`

Explanation An unexpected interrupt was reported for the specified slot and port. The specified slot will be faulted.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

BLOOM-TRNK_MSTR_DWN

Message `<switch number> Warning BLOOM-TRNK_MSTR_DWN, 3, S<slot number>, P<port number>(<blade port number>):: Trunk master port <trunk master port> goes OFFLINE in trunk group [trunk group range]`

Explanation The master trunk port is offline in the specified trunk group. The Master ISL has been physically disconnected or has failed.

Action Determine whether the Master ISL has been physically disconnected or disabled. If not, enter the `portlogdump` and `fabstateshow` commands, save the output, and contact EMC Customer Support Center for assistance.

Severity Warning

BLOOM-TRNK_SLV_DWN

Message `<switch number> Warning BLOOM-TRNK_SLV_DWN, 3, S<slot number>, P<port number>(<blade port number>): Trunk slave port <trunk slaveport> goes OFFLINE in trunk group [trunk group]\`

Explanation The slave trunk port is offline in the specified trunk group. A subordinate ISL has been physically disconnected or has failed.

Action Determine whether a subordinate ISL has been physically disconnected or disabled. If not, enter the `portlogdump` and `fabstateshow` commands, save the output, and contact EMC Customer Support Center for assistance.

Severity Warning

BLOOM-TX_PAR_FDET_ERR

Message `<switch number> Panic BLOOM-TX_PAR_FDET_ERR, 0, S<slot number>, P<port number>(<blade port number>):fdet<error message string>`

Explanation A hardware transmit failure detection error was reported for the specified slot and port.

Action Copy the error message and call Customer Support .

Severity Panic

BLOOM-TX_PARITY_ERR

Message `<switch number> Warning BLOOM-TX_PARITY_ERR, 3, S<slot number>, P<port number>(<blade port number>):tx parity error, int_status=<interrupt status>`

Explanation The indicated slot and port detected a parity error in the transmit data stream. The specified slot will be faulted.

Action Copy the error message information, run `portlogdisable` and `supportshow` (in order) to capture debug information, and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Warning

5

CFGLOADER_System Error Messages

This chapter contains the following sections:

Introduction

The Configuration Loader is the first application to run on the system. CFGLOADER's main responsibility is to determine the system platform and obtain the appropriate configuration data for other applications. After completion, CFGLOADER exits and does not run again until the next reboot.

CFGLOADER-HIL_FAIL

Message

```
<switch number> Critical, CFGLOADER-HIL_FAIL, 1, Config
   Loader failed: <failure description> (err= error
   number)
```

Explanation

The configuration loader cannot read the specified data *<failure description>*. The error number provides debugging information.

The following variables may be displayed in the *<failure description>*:

- For bladed and non-bladed switches:
  - hilGetIOXinfo - get extSysID
  - hilGetIOXinfo - get SysID
  - hilGetIPAddr - get default
  - hilGetSwName - get default
  - hilGetWWNNum - get default
- For bladed switches only:
  - hilGetNumSwitch - get default
  - hilGetChassisHA - get default
  - hilGetFruHder - WWN card has bad FRU - get default

Action

If the rest of the system initialization continues to run ok, the user may re-configure default values to the real values. If the rest of the system initialization has errors, reboot or power cycle the CP Card. Verify the CP Cards and WWN Cards are plugged in correctly. If error recurs, contact EMC Customer Support Center.

Severity

Critical

CFGLOADER-IOCTL_FAIL

Message

```
<switch number> Critical, CFGLOADER-IOCTL_FAIL, 1, Config
   Loader failed:
<failure type> <failure description>
```

Explanation The configuration loader cannot communicate with the system driver to download the system configuration. The firmware may be corrupted. The following descriptions may be displayed:

<failure type>	<failure description>
IOC_M_CLEAR_ERR	Can't drop House-Keeping Self-Fence
IOC_M_SET_NUMCP	Can't set up CP hot-plug support
sysCrtlGetCpSlot	Can't locate CP slot
IOC_SM_SET_MODEL	Can't set Platform Model information
IOC_SM_SET_CONFIG	Can't set generic configuration

Action Download new firmware and reboot.

Severity Critical

CFGLOADER-LOADER_FAIL

Message

```
<switch number> Critical, CFGLOADER-LOADER_FAIL, 1,
   Config Loader failed: <failure description>
```

Explanation

The configuration loader failed to open the system driver for communication. The failure may be due to a bad CP Card FRU; the FRU header might be corrupted or there may be i2c bus access problems resulting from a data corruption or an unsuccessful read.

The following *<failure descriptions>* may be displayed:

- sysModInit
- Config loader failed, also failed to assert CP error
- Config loader failed, assert CP error
- This CP has bad FRU (<slot number = 5 or 6>)

Action

Reboot or power cycle the switch. If problem persists, replace the CP card and reboot/power cycle again. If error recurs, contact EMC Customer Support Center.

Severity

Critical

CFGLOADER-MALLOC

Message `<switch number> Critical, CFGLOADER-MALLOC, 1, Config Loader failed: <failure description>`

Explanation Configuration loader cannot allocate any memory for its operation. The system might have a memory leak or corrupted firmware. The *<failure description>* reads as follows:

- No memory for config loader data (InitData)

Action Download new firmware and reboot. If the problem is not resolved, contact EMC Customer Support Center.

Severity Critical

CFGLOADER-UNEXPECTED_VAL

Message `<switch number> Critical, CFGLOADER-UNEXPECTED_VAL, 1, <failure description> (val=0x<value>)`

Explanation Neither HIL (the Hardware Independent Layer application) nor Configuration Loader could detect any CP Card or WWN Card in the system.

The following *<failure descriptions>* may be displayed:

- HIL detects no CP exists in the system
- Wrong Extended SystemID
- Wrong SystemID
- Invalid number of switches - get default
- There is no WWN Card in the system - no response from WWN Card
- WWN Card has no power, consider device absent - HIL and CFGLOADER read something from the WWN Card, but detect WWN Card does not have adequate power.

Action For Wrong Ext System ID and Wrong System ID: Verify the SystemID is valid.

For all other *<failure descriptions>*, verify the CP Card(s) or WWN Card, as indicated in description, are seated correctly. Power cycle the switch.

If the problem persists, replace the CP Card or WWN Card, as appropriate, or contact EMC Customer Support Center.

Severity Critical

6

CHIPS_System Error Messages

This chapter contains the following information:

Introduction

The CHIPS error messages come from the blade driver for the ASIC chip.

CHIPS-EXCESSIVE_CHIP_INT

Message

```
<switch number> Panic CHIPS-EXCESSIVE_CHIP_INT, 0, Busy
   with emb-port int. for chip <chip number> in minis
   <mini switch number> on blade <blade number>, chip
   int. is disabled. interrupt status=<interrupt status>
```

Explanation Too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the CP from becoming too busy.

Action To recover from this problem:

- On a bladed switch, perform the following commands: `slotpoweroff` *<blade number>* then `slotpoweron` *<blade number>*.
- On a non-bladed switch, reboot or powercycle the switch.

If the problem recurs, run `portlogdisable` and `supportshow` (in order) to capture debug information from these commands and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity Panic

CHIPS-EXCESSIVE_PORT_INT

Message

```
<switch number> Info CHIPS-EXCESSIVE_PORT_INT, 4, bport
   <blade port number> status=<interrupt status>
```

or

```
<switch number> Info CHIPS-EXCESSIVE_PORT_INT, 4, bport
   <blade port number> status=<interrupt status>
Port <user port number> will be re-enabled in 1 minute.
   Check cable, gbic and targets if this port is faulted
   again.
```

Explanation

The first error message example appears if the specified back-end port is faulted due to too many interrupts. The port will remain in a faulted state for one minute and will then be re-enabled.

The second error message example appears when the specified port is a front-end user port.

This problem could be caused by a bad cable, GBIC, or devices connected to the specified port.

Action

Check for faulty cable, GBIC, or devices attached to the specified port.

If the error recurs, run `portlogdisable` and `supportshow` (in order) to capture debug information from these commands and contact EMC Customer Support Center. Customer Support may also ask for additional debug information from POST and systemtest.

Severity

Info

7

DIAG_System Error Messages

This chapter contains information on the following:

Introduction

The DIAG error message module provides error messages for hardware failures. Each error message string provides the switch number, the severity level, and the name of the error message.

DIAG-ACTTEST

Message

```
<switch number> Critical DIAG-ACTTEST, 1, <test name>, pass <number>,
<port ID> Failed filter test <test number>: action type sb: <action
   name> act:<action name>
```

Explanation During filter test, the action type of the received frame is not the same action type as the sent frame. An ASIC failure is the probable cause.

Action Replace the 16-Port Card in the specified slot.

Severity Critical

DIAG-BADINT

Message

```
<switch number> Critical DIAG-BADINT, 1, <test name>, pass <number>,
<port ID> <subtest name> got interrupt,int_status=<interrupt number> when
   not expecting one
```

Explanation While running *<test name>*, the switch experienced an unexpected interrupt on pass *<number>* at the specified *<port ID>*, running *<subtest name>*. The interrupt status is defined by *<interrupt number>*. Probable cause is an ASIC failure.

Action Replace 16-Port Card containing the specified *<port ID>*.

Severity Critical

DIAG-BUS_TIMEOUT

Message

```
<switch number> Critical DIAG-BUS_TIMEOUT, 1, <test name>,
<port ID> BTO accessing <register name> Register at Address <register
   address>,
```

Explanation The ASIC register or the ASIC SRAM did not respond to an ASIC data access. The probable cause is an ASIC failure.

Action Replace 16-Port Card containing the specified *<port ID>*.

Severity Critical

DIAG-CAMINIT

Message

```
<switch number> Critical DIAG-CAMINIT, 1, <test name>, pass <number>,
<port ID> Failed to Init: <reason>
```

Explanation The specified port failed to initialize due to one of the following reasons:

- The switch not disabled.
- The diagnostic queue is absent.
- The memory allocation (MALLOC) failed.
- A chip is not present.
- The port is not in loopback mode.
- The port is not active.

Action Retry, reboot (or failover). If the problem recurs, replace the mainboard assembly.

Severity Critical

DIAG-CAMSID

Message

```
<switch number> Critical DIAG-CAMSID, 1, <test name>, pass <number>,
<port ID> <no> translation test,received <source ID>, transmitted <expected
   source ID>
```

Explanation The ASIC failed the Source ID non-translation test or the translation test. The *<source ID>* in the received frame must match the *<expected source ID>* in the transmitted data. An ASIC failure is the probable cause.

Action Replace mainboard assembly.

Severity Critical

DIAG-CANTRCV

Message

```
<switch number> Critical DIAG-CANTRCV, 1, <test name>, pass <number>,
<port ID> Cannot Receive Frame: portReceive status: <receiver status code>
   iu_status: <IU status code>
```

Explanation The port timed out; it either did not receive a message in the port receiving message queue or it returned a bad receive buffer status. An ASIC failure is the probable cause.

Action Replace the 16-Port Card containing the specified *<portID>*.

Severity Critical

DIAG-CANTXMIT

Message

```
<switch number> Critical DIAG-CAMINIT, 1, <test name>, pass <number>,
<port ID> Cannot Transmit Frame: portTransmit returns <transmitter status>
```

Explanation The specified port failed to transmit frames. An ASIC failure is the probable cause.

Action Replace the 16-Port Card containing the specified *<portID>*.

Severity Critical

DIAG-CLEARERR

Message

```
<switch number> Info DIAG-CLEARERR, 3, <port ID> Diagnostics Error Cleared
```

Explanation The diagnostic error flag (OK or BAD) for the specified port is cleared.

Action No action is required.

Severity Informational

DIAG-CMBISRF

Message

```
<switch number> Critical DIAG-CMBISRF, 1, <test name>, pass <number>, <port
   ID> <internal port number>, Ch <slot number/chip number> BISR,BIST
   Self-Test Fail,
RAMs fail bitmap: is <actual bitmap> sb <expected bitmap> er <error bitmap>
```

Explanation The ASIC central memory failed to complete the Built-in Self Repair (BISR) within the timeout period. As a result, any bad memory cells in the central memory are not repaired. When the BISR fails, the Built-in Self Test (BIST) runs automatically and will fail also. An ASIC failure is the probable cause.

Action Replace the 16-Port Card containing the specified <*portID*>.

Severity Critical

DIAG-CMBISRTO

Message

```
<switch number> Critical DIAG-CMBISRTO, 1, <test name>, pass <number>
<port ID> <internal port number>, Ch <slot number/chip number> BISR,BIST
   Timed Out,RAMs done bitmap: Err Bits <four digit bitmap>
```

Explanation The ASIC central memory failed to complete the Built-in Self Repair (BISR) within the timeout period. When the BISR fails, the Built-in Self Test (BIST) runs automatically and will fail also. An ASIC failure is the probable cause.

Action Replace the 16-Port Card containing the specified *<portID>*.

Severity Critical

DIAG-CMERRPTN

Message

```
<switch number> Critical DIAG-CMERRPTN, 1, <test name>, pass <number>,
<port ID> Offs <line offset> <CMEM error type> at wrong port, <actual port
   number> sb <expected port number>,
```

Explanation The *<central memory error type>* was detected at the wrong port *<actual port number>*, should be at the *<expected port number>*. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMERRTYPE

Message

```
<switch number> Critical DIAG-CMERRTYPE, 1, <test name>, pass <number>,
Pt <source slot/ chip (blade port) -> dest slot/chip (blade port)> Offs
   <line offset> Wrong error type. Pt <port number> is <actual error> sb
   <expected error>,
```

Explanation The destination port received the wrong central memory (CMEM) *<actual error>*; should be *<expected error>*. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMICKSUM

Message

```
<switch number> Critical DIAG-CMICKSUM, 1, <test name>, pass <number>,
<port ID> (bad | good | NOT TARGET) Cksum Test,
bit6 is <actual bit state> sb <expected bit state>, Pt<CMI error chip
   number>,
```

Explanation The CMI (Central Memory Interface) test detected checksum failure. An ASIC or 16-Port Card failure was reported. Depending on the test involved, this could happen during bad checksum test, good checksum test or NOT TARGET checksum test.

- Bad checksum test : CMI error bit <bit6> should be set in CMI error state register.
- Good checksum test : CMI error bit <bit6> should not be set in CMI error state register.
- NOT TARGET checksum test: CMI error bit <bit6> should not be set in CMI error state register.

Action Replace the ASIC or 16-Port Card.

Severity Critical

DIAG-CMIDATA

Message

```
<switch number> Critical DIAG-CMIDATA, 1, <test name>, pass <number>,
<port ID pair> RX Data is <actual data> sb <expected data> er <error bits>,
```

Explanation The CMI (Central Memory Interface) test received unexpected CMI test data <bit 0-15> from CMI self-test register.

Action Replace the ASIC or 16-Port Card.

Severity Critical

DIAG-CMIINVCAP

Message

```
<switch number> Critical DIAG-CMIINVCAP, 1, <test name>, pass <number>,
<port ID pair>: <port ID> erroneous CMI Capture Flag (bit31-1),
```

Explanation Erroneous CMI (Central Memory Interface) capture flag was detected. In other words, the CMI capture flag was set on incorrect port. The CMI capture flag located in bit 31 of a CMI self-test register indicates that a CMI self-test message was received from the CMI bus.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMINCBISR

Message

```
<switch number> Critical DIAG-CMINCBISR, 1, <test name>, pass <number>,
<port ID> inconsistent BISR result RAM# <RAM number> previous repair
   <previous solution> current repair <current solution>
```

Explanation The test *<test name>* attempted to verify that the repair solution from BISR (Built-In-Self-Repair) is consistent but the test detected an inconsistent result. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMINOCAP

Message

```
<switch number> Critical DIAG-CMINOCAP, 1, <test name>, pass <number>,
<port ID pair>: RX Pt <port ID> No CMI Capture Flag (bit31-0),
```

Explanation There is no CMI (Central Memory Interface) capture flag. An ASIC or 16-Port Card failure is the probable cause. The CMI flag indicates that a CMI self-test message was received from the CMI bus.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMISA1

Message

```
<switch number> Critical DIAG-CMISA1, 1, <test name>, pass <number>,
<port ID> TX Pt CMI Self-Test Start bit30 s-a-1,
```

Explanation The CMI (Central Memory Interface) self-test started, but "Self -Test Start flag <bit30>" has never been cleared. An ASIC failure is the probable cause. The "Self-Test Start bit" is expected to be cleared automatically once the self-test message is sent.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMNOBUF

Message

```
<switch number> Critical DIAG-CMNOBUF, 1, <test name>, pass <number>,
<port ID> No more buffers
```

Explanation The specified port could not find an available buffer for testing. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMNONPRIME

Message

```
<switch number> Critical DIAG-CMNONPRIME, 1, <test name>, pass <number>,
<port ID> BISR non-prime part
RAM# <ram number>: <repair solution> (<num> bad rows, <num> redundant rows)
```

Explanation The test <*test name*> expected to find prime ASIC parts (one without any bad rows of cells in central memory). However, it detected a number of bad rows of cells in the specified ASIC.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMRWPERR

Message

```
<switch number> Critical DIAG-CMRWPERR, 1, <test name>, pass <number>,
<port ID> RW parity error,
IntStatReg <register value> BufMemErrReg <register value>
```

Explanation The test <*test name*> detects a parity error in the interrupt status register when it is testing the central memory. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-CMTO

Message

```
<switch number> Critical DIAG-CMTO, 1, <test name>, pass <number>,
<port ID> timeout,
MEM_RUNNING bit 0 Stuck High,
```

Explanation A central memory time-out occurred during write access. The initiated data transfer did not complete within the time-out period. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-DATA

Message

```
<switch number> Critical DIAG-DATA, 1, <test name>, pass <number>,
<port ID pair> Payld Byte <index> is <actual iu data> sb <expected iu data>
```

Explanation The payload received by the specified *<port ID>* did not match the transmitted payload. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media or 16-Port Card.

Severity Critical

DIAG-DEC_RWTEST

Message

```
<switch number> Critical DIAG-DEC_RWTEST, 1, <test name>, pass <number>,
<port ID> Failed: <register name> <prerequisite flags>
r=<pattern number> c=<result flags>
```

Explanation The ASIC internal registers failed the read-modify-write operation. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-EPI1_STATUS_ERR

Message

```
<switch number> Critical DIAG-EPI1_STATUS_ERR, 1, <test name>, pass
   <number>,
<port ID> <port speed> Embedded Port Interrupt 1 Status Error: <status>
```

Explanation When the port is in force failure mode, the receiving (RX) port interrupt is in *bad finish message* error status. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-ERRSTAT

Message

```
<switch number> Critical DIAG-ERRSTAT, 1, <test name>, pass <number>,
<port ID> <counter name> Error Counter is <count> sb 0,
```

Explanation One of the ASIC internal counters *<counter name>* detected an error. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media, or 16-Port Card.

Severity Critical

DIAG-ERRSTATS

Message

```
<switch number> Error DIAG-ERRSTATS, 2, <test name>, pass <number>,
<port ID> <counter name> Error Counter is <count> sb 0,
```

Explanation An ASIC internal error counter detected an error condition. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media, or 16-Port Card.

Severity Error

DIAG-FDET_PERR

Message

```
<switch number> Critical DIAG-FDET_PERR, 1, <test name>, pass <number>,
<port ID> <port speed> Failure Detection RAM Parity Error: <status>
```

Explanation An ASIC internal failure detect memory found a parity error. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-FINISH_MSG_ERR

Message

```
<switch number> Critical DIAG-FINISH_MSG_ERR, 1, <test name>, pass <number>,
<port ID> <port speed> Finish Msg Error: <status>
```

Explanation An error was detected by the ASIC frame finish message handling logic. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-FLTINIT

Message

```
<switch number> Critical DIAG-FLTINIT, 1, <test name>, pass <number>,
<port ID> Failed to Init: <reason>
```

Explanation The specified port failed to initialize due to one of the following reasons during filter test:

- The switch not disabled.
- The diagnostic queue is absent.
- The memory allocation (MALLOC) failed.
- A chip is not present.
- The port is not in loopback mode.

Action Retry, reboot (or failover). If the problem persists, replace the 16-Port Card or the mainboard assembly.

Severity Critical

DIAG-FLTRCV

Message

```
<switch number> Critical DIAG-FLTRCV, 1, <test name>, pass <number>,
<port ID> Failed to receive frame: status: <status>
```

Explanation An error was detected by the ASIC internal CAM (Content Addressable Memory) filtering logic.

Action Replace the 16-Port Card.

Severity Critical

DIAG-FLTXMIT

Message

```
<switch number> Critical DIAG-FLTXMIT, 1, <test name>, pass <number>,
<port ID> Cannot Transmit Frame: portTransmit returns <status>
```

Explanation The specified port failed to transmit frames. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-FORCEERR

Message

```
<switch number> Critical DIAG-FORCEERR, 1, <port ID> Forced error
```

Explanation The port has been forced to an error state.

Action Run the command **diagclearerror** to clear error condition.

Severity Critical

DIAG-FTPRT_STATUS_ERR

Message

```
<switch number> Critical DIAG-FTPRT_STATUS_ERR, 1, <test name>, pass
   <number>,
<port ID> <port speed> Frame Tracking Port Status Error,
Exp: <port status> Act: <port status>,
<frame tracking> <frame tracking>
```

Explanation If the port is in force failure mode, this message indicates that incorrect frame tracking port status was found.

Action Replace the 16-Port Card.

Severity Critical

DIAG-INC_RWTEST

Message

```
<switch number> Critical DIAG-INC_RWTEST, 1, <test name>, pass <number>,
<port ID> Failed: <register name> <prerequisite flags>
r=<pattern number> c=<result flags>
```

Explanation ASIC internal registers failed read-modify-write operation. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-INIT

Message

```
<switch number> Critical DIAG-INIT, 1, <test name>, <subtest name> pass
   <number>,
<port ID> <port speed> Failed to go active after initialization,
```

Explanation The port failed to go active in the loopback mode requested. Fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace fibre cable, media, or 16-Port Card.

Severity Critical

DIAG-INTNIL

Message

```
<switch number> Critical DIAG-INTNIL, 1, <test name>, pass <number>,
<port ID> Failed to get CMI Error (interrupt),
```

Explanation The port failed to go active in the loopback mode requested. Fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace fibre cable, media, or 16-Port Card.

Severity Critical

DIAG-INTNOTCLR

Message

```
<switch number> Critical DIAG-INTNOTCLR, 1, <test name>, pass <number>,
<port ID> Offs <ram offset> CMEM_ERR int bit could not be cleared,
```

Explanation The interrupt bit could not be cleared. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-LCMEM

Message

```
<switch number> Critical DIAG-LCMEM, 1, <test name>, pass <number>,
<port ID> Wr/Rd,
bNum <bad buffer> bLine <bad line> Offs <offset> error bits <bit mask>
```

Explanation The data read from the central memory location did not match data previously written into the same location. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-LCMEMTX

Message

```
<switch number> Critical DIAG-LCMEMTX, 1, <test name>, pass <number>,
<port ID pair> Tx Rd,
Wd <bad word> error bits <bit mask>
```

Explanation A central memory transmit path failure was detected. First ASIC in *<port ID pair>* failed to read the second ASIC in *<port ID pair>* using the transmit path. A 16-Port Card failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-LCMTO

Message

```
<switch number> Critical DIAG-LCMTO, 1, <test name>, pass <number>,
<port ID> timeout,
MEM_RUNNING bit 0 Stuck High,
```

Explanation A central memory time-out was reported. The initiated data transfer did not complete within the time-out period. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-LESSN_STATUS_ERR

Message

```
<switch number> Critical DIAG-LESSN_STATUS_ERR, 1, <test name>, pass
   <number>,
<port ID> <port speed> Buffer Tags Status Error,
Exp: <expected status> Act: <actual status>
```

Explanation If the switch is in force failure mode, the less_n register has bad buffer tags error status. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

Severity Error

Action

Severity Info

DIAG-MBUF_STATE_ERR

Message

```
<switch number> Critical DIAG-MBUF_STATE_ERR, 1, <test name>, pass <number>,
<port ID> <speed> Minibuffer State Checking Error: <value>
```

Explanation An ASIC pair buffer state checking error was reported. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-MBUF_STATUS_ERR

Message

```
<switch number> Critical DIAG-MBUF_STATUS_ERR, 1, <test name>, pass
   <number>,
<port ID> <speed> Minibuffer State Checking Status Error,
Exp: <expected value> Act: <actual value>
```

Explanation If the switch is in force failure mode, a bad minibuffer state checking status found.

Action Replace the 16-Port Card.

Severity Critical

DIAG-NOSEGMENT

Message

```
<switch number> Critical DIAG-NOSEGMENT, 1, <test name> <subtest name>,
<port ID> <speed> Failed to segment,
Please check cables
```

Explanation The specified port failed to go into loopback mode. An improper media or cable connection is the likely cause.

Action Reset the specified media and cables, then re-execute test.

Severity Critical

DIAG-NUMTEST

Message

```
<switch number> Critical DIAG-NUMTEST, 1, <test name>, pass <number>,
<port ID> Failed filter test #<test number>: filter number sb: <expected
   number> act: <actual number>
```

Explanation The wrong filter number changed states during the filter test. An improper media or cable connection is the likely cause.

Action Reset the specified media and cables, then re-execute test.

Severity Critical

DIAG-PORTDIED

Message

```
<switch number> Critical DIAG-PORTDIED, 1, <test name> <subtest name>, pass
   <number>,
<port ID> <speed> Was Active but Went Inactive (Offline),
```

Explanation The specified port was in loopback mode and then went inactive. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media, or 16-Port Card/ASIC.

Severity Critical

DIAG-PORTENABLE

Message

```
<switch number> Critical DIAG-PORTENABLE, 1, <test name> <subtest name>,
   pass <number>,
<port ID> <speed> Failed enable.
```

Explanation An ASIC driver detected an error when attempting to bring the port online. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media, or 16-Port Card/ASIC.

Severity Critical

DIAG-PORTM2M

Message

```
<switch number> Critical DIAG-PORTM2M, 1, <test name>,
<port ID> Port M->M Connection not allowed,
```

Explanation The specified port is found to be connected to itself (self loopback). The Port M to Port M connection is not allowed by the test. An improper cable connection is the likely cause.

Action Reconnect port (M) to another port (N) and re-execute the test.

Severity Critical

DIAG-PORTSTOPPED

Message

```
<switch number> Critical DIAG-PORTSTOPPED, 1, <test name>, <number> nMegs,
<port ID> No Longer Transmitting, FTX Counter Stuck at <counter value>
```

Explanation The specified port is no longer transmitting frames. The Number Of Frames Transmitted counter is stuck at *<counter value>*. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media, or 16-Port Card/ASIC.

Severity Critical

DIAG-PORTWRONG

Message

```
<switch number> Critical DIAG-PORTWRONG, 1, <test name>, pass <number>,
Frame Received at Wrong Port: is <port ID> sb <port ID>
```

Explanation A frame was erroneously received by port M instead of the intended port N. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-REGERR_UNRST

Message

```
<switch number> Critical DIAG-REGERR_UNRST, 1, <test name>,
<port ID> 3 retries,
lli_ctl <actual value> sb 90000, port_config <actual value> sb <expecteed
   value>
```

Explanation The specified port failed to reset despite three retries. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-RXQ_FRAME_ERR

Message

```
<switch number> Critical DIAG-RXQ_FRAME_ERR, 1, <test name>, pass <number>,
<port ID> <speed> RX Queuing Frame Tracking Number Error: <value>
```

Explanation A data error was detected in the receiving (RX) port queuing memory.

Action Replace the 16-Port Card.

Severity Critical

DIAG-RXQ_RAM_PERR

Message

```
<switch number> Critical DIAG-RXQ_RAM_PERR, 1, <test name>, pass <number>,
<port ID> <speed> RX Queuing RAM Parity Error: <value>
```

Explanation A parity error was detected in the receiving (RX) queuing RAM of the ASIC.

Action Replace the 16-Port Card.

Severity Critical

DIAG-SMI_STUCK

Message

```
<switch number> Warning DIAG-SMI_STUCK, 3, <port ID> stuck at SMI OP still
  running
```

Explanation The status indicator of the ASIC Special Memory Interface (SMI) is stuck on the specified port.

Action Replace the 16-Port Card.

Severity Warning

DIAG-STATS

Message

```
<switch number> Critical DIAG-STATS, 1, <test name>, pass <number>,
<port ID> <counter name> Counter Wrong, is <actual value> sb <expected
   value>
```

Explanation The ASIC internal error counters detected an error condition. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical .

DIAG-STSALPACNT

Message

```
<switch number> Critical DIAG-STSALPACNT, 1, <test name>, pass <number>,
<port ID> Failed ALPA stat counter test:
alpa(<address>) status count exp:<expected value> act:<actual value>
```

Explanation An incorrect ALPA count found. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-STSINIT

Message

```
<switch number> Critical DIAG-STSINIT, 1, <test name>, pass <number>,
<port ID> Failed to Init: <reason>
```

Explanation One of two problems may have caused the reported error:

- The space for frames could not be allocated.
- The port failed to initialize.

The problem may be due to an ASIC failure.

Action Replace the 16-Port Card.

Severity Critical

DIAG-STSNULL

Message

```
<switch number> Critical DIAG-STSNULL, 1, <test name>, pass <number>,
<port ID>
ptRegs(pt): Null pointer detected
```

Explanation An error occurred while sending data or a bad port number was detected.

Action Replace the 16-Port Card.

Severity Critical

DIAG-TIMEOUT

Message

```
<switch number> Critical DIAG-TIMEOUT, 1, <test name>, pass <number>,
<port ID> Receive Error | Timeout
status rx: <value>, iu: <value>
```

Explanation The specified port failed to detect an interrupt within the time-out period. A fibre cable, media, or 16-Port Card/ASIC failure is the probable cause.

Action Replace the fibre cable, media, or 16-Port Card/ASIC.

Severity Critical

DIAG-WTEST

Message

```
<switch number> Critical DIAG-WTEST, 1, <test name>, pass <number>,
<port ID> Failed: <register name>
w=<write pattern> c=<control value>
```

Explanation The ASIC internal registers failed the write operation. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

DIAG-XMIT

Message

```
<switch number> Critical DIAG-WTEST, 1, <test name>, pass <number>,
<port ID> Cannot Transmit Frame: diagPtRegister returns <return value>
```

Explanation The specified port failed to transmit frame. An ASIC failure is the probable cause.

Action Replace the 16-Port Card.

Severity Critical

8 ERRLOG_System Error Messages

This chapter contains the following sections:

Introduction

The Error Log subsystem collects information about the systems' health as well as warning or information conditions from various subsystems. The Error Log subsystem then displays the collected information in text format on the system console and stores required error messages in non-volatile storage so the information can be retrieved and displayed later.

ERRLOG-LOGCLRD

Message

```
<switch number> Info ERRLOG-LOGCLRD, 4, Error log cleared
```

Explanation Informational message stating that the error log was cleared using the telnet command `errclear`.

Recommended Action No action required. Information only.

Severity Info

ERRLOG-NV_DISABLE

Message

```
<switch number> Info ERRLOG-NV_DISABLE, 4, Persistent error log will be
  disabled soon...
```

Explanation An informational message stating that the Persistent (Non-Volatile) Error Log will be disabled by the telnet command `errnvlogdisable` issued by the user.

Action No action required. Information only.

Severity Info

ERRLOG-NV_LOG_CLRD

Message

```
<switch number> Info ERRLOG-NV_LOG_CLRD, 4, Persistent error log cleared
```

Explanation An informational message stating that the Persistent (Non-volatile) Error Log has been cleared with the `errClear -p` command.

Action No action required. Information only.

Severity Info

ERRLOG-NV_LOG_RESIZE

Message

```
<switch number> Info ERRLOG-NV_LOG_RESIZE, 4, Persistent error log is
  resized to <number of errors in log> entries
```

Explanation An informational message stating that the number of errors in the Persistent (Non-volatile) Error Log has been changed and can now store *<number of errors in log>* entries. The default size is 1024, and can be re-sized to any value between 1024 and 2068.

Action No action required. Information only.

Severity Info

ERRLOG-SET_MSG_SAVE_LVL

Message

```
<switch number> Info ERRLOG-SET_MSG_SAVE_LVL, 4, Error Log message save
   level is set to <error level>
```

Explanation An informational message stating the level of error that is set to be saved in the Persistent (Non-volatile) Error Log. For example, if the level is set to 3, then 0, 1, 2, and 3 level error messages will be stored.

The maximum number of persistent messages is 256, therefore it is recommended that you set the number to record lower (or more critical errors) such as 0 and 1. However, if the log fills up, more critical messages will always take precedence over less critical messages in the log.

The levels of error messages are:

0 Panic
1 Critical
2 Error
3 Warning
4 informational
5 Debug

Action No action required. Information only.

Severity Info

9 FABRIC_System Error Messages

This chapter contains the following sections:

Introduction

FABRIC refers to a network of fibre channel switches. The FABRIC error messages come from the fabric daemon. Fabricd implements the Fibre Channel Switch Fabric (FCSF) standard. Fabricd follows the FCSF standard for the fabric initialization process such as determining the E_ports, assigning unique domain ID to switches, creating a spanning, tree, throttling the trunking process, and distributing the domain and alias list to all switches in the fabric.

FABRIC-ASYNC

Message

```
<switch number> Warning FABRIC-ASYNC, 3, port: <port number>, req iu: <IU
   sent>, state: <command sent>, resp iu: <response IU>, state <response IU
   state> "unexpected resp async state"
```

Explanation The Information Unit response was invalid for the specified command sent.

Action Copy error message and call Customer Support .

Severity Warning

FABRIC-ASYNC_COMMAND

Message

<switch number> Warning FABRIC-ASYNC_COMMAND, 3, Command: port *<port number>*: status *<reason for failure>* (Reason for failure) xid = *<exchange ID of command>*

Explanation The application failed to send an async command for the specified port.The message provides additional details regarding reason for failure and exchange ID for the command.

Action Run the `supportshow` command and call Customer Support .

Severity Warning

FABRIC-BADILS

Message

<switch number> Warning *FABRIC-BADILS, 3, port <port number>: ILS <command> bad size <payload size>, wanted <expected payload size>*

Explanation A Switch Fabric Internal Link Service (ILS) IU of invalid size has been received.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_BF

Message

<switch number> Info *FABRIC-FAB_BF, 4, <reconfiguration description>*

Explanation The fabric reconfiguration during "build fabric" transitions to the "F0: Non-disruptive state" (F0 state details provided in the Fibre Channel Switch Fabric specification).

Action No action required.

Severity Info

FABRIC-FAB_EFP_ERROR

Message

<switch number> Warning *FABRIC-FAB_EFP_ERROR, 3, <error description>*

Explanation Errors were reported during the Exchange Fabric Parameter state; cannot allocate domain list due to a bad EFP type.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_FWD_ERROR

Message

```
<switch number> Warning FABRIC-FAB_FWD_ERROR, 3, <error description>
```

Explanation Errors occurred while forwarding RDI (Request Domain ID) commands to the upstream link; cannot cleanup the IU. Error description provides further details.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_IU_FREE

Message

```
<switch number> Warning FABRIC-FAB_IU_FREE, 3, IU free error, caller:
  <function attempting to de-allocate IU>
```

Explanation A failure occurred when freeing or de-allocating an IU.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_ME_ERROR

Message

```
<switch number> Error FABRIC-FAB_ME_ERROR, 2, <error description>
```

Explanation Unable to inform FSSME (Fabric OS State Synchronization Management Module) that the fabric is stable or unstable.

Action Run `supportshow` and `hadump` then contact EMC Customer Support Center.

Severity Error

FABRIC-FAB_NODE_FREE

Message

```
<switch number> Warning FABRIC-FAB_NODE_FREE, 3, Node free error, caller:
  <error description>
```

Explanation This message occurs when the application tries to free or de-allocate memory space that has already been de-allocated.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_PERSIST_DID_FAIL

Message

```
<switch number> Error FABRIC-FAB_PERSIST_DID_FAIL, 2, Port <port number>
   Disabled: Persistent Domain ID <Domain ID> could not be obtained.
   Principal Assigned Domain ID = <Domain ID>
```

Explanation The specified port received an RDI (Request Domain ID) Accept message containing the Principal Assigned Domain ID which is different from the Persistent Domain ID. Therefore, the port is disabled.

Action No action required.

Severity Error

FABRIC-FAB_PERSIST_ISOLATE

Message

```
<switch number> Error FABRIC-FAB_PERSIST_ISOLATE, 2, Persistent DID max
   retry exceeded: All E-Ports will be disabled.
   Switch is isolated.
```

Explanation The application exceeded RDI (Request Domain ID) requests for the Persistent Domain ID. All E_ports will be disabled, thereby isolating the specified switch from the fabric.

Action Verify the Persistent Domain ID is unique in the fabric, then re-enable the E_ports. If error persists, run `supportshow` and contact EMC Customer Support Center.

Severity Error

FABRIC-FAB_PSS_PRINCIPAL_FAIL

Message

```
<switch number> Warning FABRIC-FAB_PSS_PRINCIPAL_FAIL, 3, PSS principal
  failed (reason for failure>: <WWN of new principal switch>)
```

Explanation The message will only display if the switch is configured to be the principal switch when using the `fabricprincipal` command. The message notifies user that the switch failed to become the principal switch because the switch either joined an existing fabric and bypassed the F0 State, or the switch lost to another switch that is also configured to be the principal switch and has a lower WWN.

Action No action required.

Severity Warning

FABRIC-FAB_RDI_ERROR

Message

```
<switch number> Warning FABRIC-FAB_RDI_ERROR, 3, <error description>
```

Explanation Errors occurred during the Request Domain ID state; IU cannot be allocated/sent.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_TYPE_ERROR

Message

<switch number> Warning FABRIC-FAB_TYPE_ERROR, 3, *<function stream>*: no such type, *<invalid type>*

Explanation The fabric is not in the appropriate state for the specified process.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Warning

FABRIC-FAB_VAL_DOM

Message

<switch number> Info FABRIC-FAB_VAL_DOM, 4, *<valid domain>*

Explanation The fabric Domain ID is found to be valid.

Action No action required.

Severity Info

FABRIC-NO_ALIASID

Message

```
<switch number> Warning FABRIC-NO_ALIASID, 3, fabGaid: no free multicast
  alias IDs
```

Explanation The fabric does not have available multicast alias IDs to assign to the alias server.

Action Verify Alias IDs using the `fabricshow` command on the principal switch.

Severity Warning

FABRIC-SEGMENTED

Message

```
<switch number> Warning FABRIC-SEGMENTED, 3, port <port number>,
  <description of segmentation>
```

Explanation The port is segmented from neighboring switch. Error message provides additional description and information regarding segmentation.

Action Verify that specified port is segmented using the command `switchshow`. Using information provided in *<description of segmentation>*, resolve the reason for segmentation.

Severity Warning

FABRIC-SIZE_EXCEEDED

Message

```
<switch number> Critical FABRIC-SIZE_EXCEEDED, 1, "Critical fabric size
   <number of switches in fabric> exceeds configuration <number of allowed
   switches> Switch status marginal. Contact Technical Support."
```

Explanation Too many switches in the fabric.

Action Reduce size of fabric. Remove switches until number of switches meet supported configuration. contact EMC Customer Support Center with any questions.

Severity Critical

FABRIC-WEBTOOL_LIFE

Message

```
<switch number> Critical FABRIC-WEBTOOL_LIFE, 1, Webtool will be disabled in
   <number> days and <number> hours and <number> minutes
```

Explanation If the fabric size exceeds the supported configuration, then WebTools will be disabled in the specified number of days, hours, and minutes.

Action The user must remove switches from the fabric until the fabric meets the supported configuration

Severity Critical

FABRIC-WEBTOOL_DISABLE

Message

```
<switch number> Critical FABRIC-WEBTOOL_DISABLE, 1, Webtool is disabled.
```

Explanation WebTools is disabled until fabric size meets supported configuration.

Action Remove switches from the fabric until the fabric meets the supported configuration. WebTools will automatically function.

Severity Critical

10 FCIU_System Error Messages

This chapter contains the following information:

Introduction

FCUI stands for Fibre Channel Information Unit. The FCIU error messages are reported from the FCPH (Fibre Channel Physical and Signaling Interface) layer of code. The FCPH layers of code are FC-0, FC-1, and FC-2 of the Fibre Channel protocol.

FCIU-IUBAD

Message

```
<switch number> Debug FCIU-IUBAD, 5, invalid iu <IU pointer>
```

Explanation An invalid IU (information unit) was reported. The *<IU Pointer>* provides a pointer to the IU causing the error message. This error message may be caused by one of the following conditions:

- NULL IU pointer
- NULL IU header pointer
- NULL IU data pointer or no IU data
- Size of the IU is larger than the memory allocation size

Action Run the `supportshow` command to display the error message trace information that shows where the IU error message occurred. Also, copy the traceback information printed out with this error. contact EMC Customer Support Center with both sets of information.

Severity Debug

FCIU-IUCOUNT

Message

```
<switch number> Critical FCIU-IUCOUNT, 1, count <0 iu <IU Pointer>
```

Explanation The number of Information Units in use (allocated) are less than zero, but a task or application is trying to return an IU; this return is an invalid action.The *<IU Pointer>* provides a pointer to the IU causing the error message.

Action Run the `supportshow` command to find the error message trace information to see where the IU error message occurred. Also, copy the traceback information printed out with this error. contact EMC Customer Support Center with both sets of information.

Severity Critical

11

FCMISC_System Error Messages

This chapter contains the following sections:

Introduction

Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.

FCMISC-OUT_OF_MEMORY

Message

```
<switch number> Critical FCMISC-OUT_OF_MEMORY, 1, <function>:<failed
   function call> out of memory condition
```

Explanation The switch is low on memory and failed to allocate new memory for an Information Unit.

The <*function*> will be "misc_tx_lb".

The <*failed function call*> will be "iu_alloc failed". This function call is for memory allocation for information units.

Action A non-bladed switch will automatically reboot. For a bladed switch, the active CP card will automatically failover, and the standby CP will become the active CP. contact EMC Customer Support Center.

Severity Critical

12 FCP_System Error Messages

This chapter contains the following information:

Introduction

The Fibre Channel Protocol (FCP) application is responsible for probing the devices attached on the loop port. Probing is a process the switch uses to find out the devices attached on the loop ports and to update the Name Server with the information.

FCP-PROBE_TIMEOUT

Message

```
<switch number> Warning FCP-PROBE_TIMEOUT, 3, AL_PA <ALPA address> on port
   <port number> did not respond
```

Explanation FCP switch probe devices on loop port, and probing timed out on the specified port for the specified ALPA address.

Port number values may be 0-15; alpha arbitrated loop physical address range: is any value 00 - FF.

Action Retry action. If error persists, contact EMC Customer Support Center.

Severity Warning

13

FCPD_System Error Messages

This chapter contains the following information:

Introduction

The Fibre Channel Protocol (FCP) application is responsible for probing the devices attached on the loop port. Probing is a process the switch uses to find out the devices attached on the loop ports and to update the Name Server with the information:

FCPD-PROBING_FAIL

Message

```
<switch number> Warning FCPD-PROBING_FAIL, 3, Probing failed on <L-port or
   F-port> <port number> [ALPA <alpa address>]
```

Explanation FCP switch probe devices on loop port, and probing failed on the either the L-Port/ALPA address or the F-port.

Ports will be 0-63 for bladed system, terminator will be ports numbers 0-15; alpa arbitrated loop physical address: range is any value 00 - FF.

Action This can happens when the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

Severity Warning

FCPD-PORT_BAD_RCTL

Message

```
<switch number> Warning FCPD-PORT_BAD_RCTL, 3, PORT <port number>, bad R_CTL
   for fcp probing: <R_CTL value>
```

Explanation The response frame received on the specified port for a probing inquiry request contains invalid value in the routing control field.

Action This can only happen if the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix. contact EMC Customer Support Center.

Severity Warning

14 FCPH_System Error Messages

This chapter contains the following information:

Introduction

Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch. Fibre Channel Physical (FCPH) layer error messages are a result of "exchange" errors. Exchanges are the exchange of information units with identification and management mechanisms, a basic "hand-shaking", between two fibre channel ports.

FCPH-EXCHBAD

Message

```
<switch number> Critical FCPH-EXCHBAD, 1, bad xid <Exchange ID>, x:
   <Exchange Data0>, <Exchange Data1>, <Exchange Data2>, <Exchange Data3>,
   <Exchange Data4>, <Exchange Data5>, <Exchange Data6> [iu: <IU POinter>;
   header: <IU Header0>, <IU Header1>, <IU Header2>, <IU Header3>]
```

Explanation A bad (invalid) exchange ID was reported.

The following information is provided in the error message:

- *<Exchange Data0>* - The fibre channel header exchange ID for the Originator (O) and Responder (R): format [OOOORRRR].
- *<Exchange Data1>* - The fibre channel source ID.
- <Exchange Data2> - The fibre channel responder ID.
- *<Exchange Data3>* - The exchange status flags.
- *<Exchange Data4>* - The physical port number.
- *<Exchange Data5>* - The fibre channel class of service.
- *<Exchange Data6>* - The receiver unsolicited registry index.
- *<IU Pointer>* - The pointer Information Unit.
- *<IU Header0>* - The fibre channel routing control bits (R)_ and destination ID (D): format [RRDDDDDD].
- *<IU Header1>* - The fibre channel destination ID (D) and unused bits (X): format [XXDDDDDD].
- *<IU Header2>* - The fibre channel header fields type (T) and frame control (F): format {TTFFFFFF].
- *<IU Header3>* - The fibre channel header fields sequence ID, Data Field Control, and Sequence Count.

Action Run the `supportshow` command; the error message trace information will show where the IU error message occurred. Also, copy the traceback information printed out with this error. contact EMC Customer Support Center with both sets of information.

Severity Critical

FCPH-EXCHFREE

Message

```
<switch number> Debug FCPH-EXCHFREE, 5, xid <Exchange ID> free, x: <Exchange
  Data0>, <Exchange Data1>, <Exchange Data2>, <Exchange Data3>, <Exchange
  Data4>, <Exchange Data5>, <Exchange Data6>, <Exchange Data7> iu: unknown
```

Explanation The exchange ID has already been freed.

The following information is provided in the error message:

- *<Exchange Data0>* - The fibre channel header exchange ID for the Originator (O) and Responder (R): format [OOOORRRR].
- *<Exchange Data1>* - The fibre channel source ID.
- <Exchange Data2> - The fibre channel responder ID.
- *<Exchange Data3>* - The exchange status flags.
- *<Exchange Data4>* - The physical port number.
- *<Exchange Data5>* - The fibre channel class of service.
- *<Exchange Data6>* - The receiver unsolicited registry index.
- *<IU Pointer>* - The pointer Information Unit.
- *<IU Header0>* - The fibre channel routing control bits (R)_ and destination ID (D): format [RRDDDDDD].
- *<IU Header1>* - The fibre channel destination ID (D) and unused bits (X): format [XXDDDDDD].
- *<IU Header2>* - The fibre channel header fields type (T) and frame control (F): format [TTFFFFFF].
- *<IU Header3>* - The fibre channel header fields sequence ID, Data Field Control, and Sequence Count.

Action Run the `supportshow` command; the error message trace information will show where the IU error message occurred. Also, copy the traceback information printed out with this error. contact EMC Customer Support Center with both sets of information.

Severity Debug

FCPH-OUT_OF_MEMORY

Message

```
<switch number> Critical FCPH-OUT_OF_MEMORY, 1, <function>:<failed function
   call> out of memory condition
```

Explanation The switch is low on memory and failed to allocate new memory for a Fibre Channel Driver instance.

The <*function*> will be "fc_create". This function creates a Fibre Channel driver instance.

The < *failed function call*> will be "kmalloc_wrapper failed". This function call is for kernel memory allocation.

Action A non-bladed switch will automatically reboot. For a bladed switch, the active CP card will automatically failover, and the standby CP will become the active CP. contact EMC Customer Support Center.

Severity Critical

15 FLOOD_System Error Messages

This chapter contains the following information:

Introduction

FLOOD is a part of the FSPF (Fabric Shortest Path First) protocol that handles synchronization of the Link State Database (LSDB) and propagation of the Link State Records (LSR).

FLOOD-INVLSR

Message

```
<switch number> Warning FLOOD-INVLSR, 3, Unknown LSR type: port <port
   number>, type <LSR header type>
```

Explanation The Link State Record (LSR) type is unknown. The following two LSR header types are the only known types: 1 - Unicast and 3 - Multicast.

Action The record will be discarded. No user action is required.

Severity Warning

FLOOD-LINKCNT

Message

```
<switch number> Warning FLOOD-LINKCNT, 3, Link count exceeded in received
   LSR, value = <link count number>
```

Explanation The acceptable link count received was exceeded in the Link State Record.

Action The record will be discarded. No user action is required.

Severity Warning

16 FSPF_System Error Messages

This chapter contains the following information:

Introduction

Fabric Shortest Path First (FSPF) is a link state routing protocol which is used to figure out how frames should be routed. These error messages cover protocol errors.

FSPF-INPORT

Message

```
<switch number> Error FSPF-INPORT, 2, Input Port <port number> out of range
```

Explanation The specified input port number is out of range. The specified input port number does not exist on the switch.

Recommended Action Frame will be discarded and no user action is required.

Severity Error

FSPF-NBRCHANGE

Message

```
<switch number> Info FSPF-NBRCHANGE, 4, Wrong neighbor ID <port number> in
  Hello
```

Explanation Wrong Domain ID from neighbor (adjacent) switch in Hello message from specified port. This may happen when a Domain ID for a switch has been changed.

Action No user action required.

Severity Info

FSPF-REMDOMAIN

Message

```
<switch number> Error FSPF-REMDOMAIN, 2, Remote Domain ID <domain number>
   out of range, input port = <port number>
```

Explanation The specified remote Domain ID is out of range.

Action Frame will be discarded and no user action is required.

Severity Error

FSPF-SCN

Message

```
<switch number> Warning FSPF-SCN, 3, Illegal SCN, port <port number>, state
   <state code>
```

Explanation An invalid Switch Change Notification (SCN) was reported for the specified port. The only valid SCNs are: 1 (on line), 2 (off line), 3 (testing), 4 (faulty), 5 (E_Port), 6 (F_Port), 7 (segmented), 8 (T_Port).

Action SCN will be ignored. No user action is required.

Severity Warning

FSPF-SECTION

Message

```
<switch number> Error FSPF-SECTION, 2, Wrong Section Id <section number>,
  should be 0, input port = <port number>
```

Explanation An incorrect section ID was reported from the specified input port. EMC only supports Section ID 0 (zero).

Action Verify the reported Section ID is 0 (zero).

Severity Error

FSPF-VERSION

Message

```
<switch number> Error FSPF-VERSION, 2, FSPF Version <FSFP version> not
  supported, input port = <port number>
```

Explanation The FSPF version is not supported on the specified input port.

Action Update the FSPF version by loading the correct version of firmware.

Severity Error

17 FSS_System Error Messages

This chapter contains the following information:

Introduction

The Fabric OS State Synchronization framework (FSS) provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take over control of the switch non-disruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions enabling the transition from standby to active operation.

FSS is defined as a component and a service. A component is a module in the Fab OS implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.

FSS-NOMEMORY

Message

```
<switch number> Warning FSS-NOMEMORY, 3, Memory shortage
```

Explanation System ran out of memory.

Action Call Tech Support.

Severity Warning

FSS-NOTXBEGIN

Message

```
<switch number> Warning FSS-NOTXBEGIN, 3, <component name>: Missing first TX
   update <transaction id>
```

Explanation FSS dropped this transaction state update because the transaction flag was not setup.

Action Run the command `hasyncstart` on the active CP or call Tech Support.

Severity Warning.

FSS-TXTOOMANY

Message

```
<switch number> Warning FSS-TXTOOMANY, 3, <component name>: Too many
   concurrent TX <transaction id>
```

Explanation The specified component sent too many transactions at the same time.

Action System will continue to function normally. If you have any questions, call Customer Support .

Severity Warning

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ANEXO SWITCH TIPO 03
PARTE 10/B

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

18 FSSME_System Error Messages

This chapter contains the following information:

Introduction

FSSME is a management module for FSS (Fabric OS State Synchronization framework). FSSME controls FSS. FSSME is defined as a component and a service. A component is a module in Fab OS implementing a related set of funtionality. A service is a collection of components grouped together to achieve a modular software architecture.

FSSME-HA_IN_SYNC

Message

```
<switch number> Info FSSME-HA_IN_SYNC, 4, HA State is in sync!
```

Explanation This message is logged when the HA state for FabOS is in synchronization with the peer CPs' HA state. If the standby CP is healthy, then the failover would be non-disruptive. (For details on non-disruptive failover, see the *Fabric OS Command Reference v. 4.1.*)

Recommended Action No action required.

Severity Information

FSSME-HA_OUT_OF_SYNC

Message

```
<switch number> Info FSSME-HA_OUT_OF_SYNC, 4, HA State out of sync!
```

Explanation This message is logged when the HA state for FabOS is out of synchronization with the peer CPs' HA state. If the active CP were to failover when the HA state is out of sync, failover would be disruptive.

Action If this message was logged as a result of a user initiated action (such as issuing `switchreboot` or `hareboot` commands), then no action is required.

Otherwise, issue the `hasyncstart` command on the active CP and try re-synchronizing the HA state. If the HA state does not become synchronized, then run the `hadump` command and contact EMC Customer Support Center.

Severity Information

FSSME-PEER_SVC_NOT_IN_OPR

Message

```
<switch number> Info FSSME-PEER_SVC_NOT_IN_OPR, 4, Peer service not in
  operation: <service name>:<service instance>
```

Explanation This message is logged when the peer service is not in operation. When a CP is rebooted, the peer CP will print this message. This message is for technical assessment.

Action If this message is logged as a result of user action (such as `reboot` the Peer CP), then no action is required.

If this message is logged without any intentional actions as mentioned above, please run the `hadump` command and contact EMC Customer Support Center.

Severity Information

FSSME-PEER_COMP_SYNCFAIL

Message

```
<switch number> Info FSSME-PEER_COMP_SYNCFAIL, 4, Peer Component failed to
  sync <service name:<service instance>
```

Explanation This message is logged when the peer service failed to synchronize and means non-disruptive HA failover is not possible. This message provides details for technical assessment.

Action Issue `hasyncstart` command on the active CP. If this message appears again, run the `hadump` command and contact EMC Customer Support Center.

Severity Information

FSSME-PEER_COMP_NOT_IN_OPR

Message

```
<switch number> Critical FSSME-PEER_COMP_NOT_IN_OPR, 1, Peer component not
  in operation: <service name>:<service instance>
```

Explanation This message is logged when the peer component is not in operation and means non-disruptive HA failover is not possible. This message provides details for technical assessment.

Action contact EMC Customer Support Center.

Severity Critical

FSSME-LOCAL_COMP_SYNCFAIL

Message

```
<switch number> Critical FSSME-LOCAL_COMP_SYNCFAIL, 1, Local Component
  failed to sync <service name>:<service instance>
```

Explanation This message is logged when the local component failed to synchronize and means non-disruptive HA failover is not possible. This message provides details for technical assessment.

Action Issue `hasyncstart` command on the active CP. If this message appears again, run the `hadump` command and contact EMC Customer Support Center.

Severity Critical

FSSME-IMAGE_MISMATCH

Message

```
<switch number> Critical FSSME-IMAGE_MISMATCH, 1, One or more components on
   the standby and active are incompatible
```

Explanation This message is logged when there is a version mismatch between the active and standby peer components. This message provides details for technical assessment.

Action Run the `hadump` command and contact EMC Customer Support Center.

Severity Critical

19 HAM_System Error Messages

This is a BodyFirst tag. It is only used on the first paragraph in each chapter or appendix. Aside from the dramatic Space Before, it resembles, in every way, its more common relative, Body.

Set first chapter numbering to start at 1, `Numeric` format. Set subsequent and adjacent chapter numbering to `Continue numbering from previous file in book`. If chapters are separatred by pats, you'll need to enter the correct chapter number in the first filee that follows the part page.

- This is a ChapContents, which should never be typed in.
- Only use a cross reference here, like in the following:
- Introduction 19-2

Introduction

HAM is a user space daemon responsible for High Availability (HA) Management.

HAM-HMON

Message

```
<switch number> Information HAM-HMON, 4, Standby CP is Healthy
```

Explanation All of the standby CP devices monitored by Health Monitor report no error.

Action No action required.

Severity Information

HAM-HMON_FAULT

Message

```
<switch number> Critical HAM-HMON_FAULT, 1, Standby CP is not healthy,
  device <device name> status BAD severity = <severity>
```

Explanation A standby CP device error is reported by the HAM Health Monitor with specific device and severity level. The severity level may be on of the following: critical, major, minor.

The active CP will continue to function normally, but because the standby CP is not healthy, non-disruptive failover is not possible

Action Replace standby CP. Call Tech Support if necessary.

Severity Critical

HAM-ERROR

Message

```
<switch number> Critical HAM-ERROR, 4, <error message>
```

Explanation This message is logged when HAM encounters a critical error.

Action Run the `hadump` command and capture output, then call Customer Support .

Severity Critical

HAM-REBOOT_REASON

Message

```
<switch number> Info HAM-REBOOT_REASON, 4, Switch reboot, reason: unknown
```

Explanation This message is logged when HAM does not have any knowledge about the reason for switch reboot.

Action No action required.

Severity Information

20 HAMKERNEL_System Error Messages

This chapter contains the following information:

Introduction

This is the kernel module for HAM, the High Availability Management daemon.

HAMKERNEL-ERROR

Message

```
<switch number> Info HAMKERNEL-ERROR, 4, <error information>
```

Explanation This message is logged when a system error has occurred. The *<error information>* indicates where the problem is, and is used for troubleshooting.

Action Copy the error message, run the `haDump` command, and contact EMC Customer Support Center with the information.

For bladed switches, run the `haDump` command on both CP Cards.

Severity Information

HAMKERNEL-ERROR_NOTIFICATION

Message

```
<switch number> Info HAMKERNEL-ERROR_NOTIFICATION, 4, Error notification
  received: <error information>
```

Explanation The High Availability Manager Kernel has been notified of an error in the system. The source error itself will be logged before this message is logged. Depending on the severity of the error logged, the High Availability Manager will reboot or failover, depending on the platform.

Recommended Action Run `haDump` and `errDump`, for Silk Worm 12000 obtain the output of `haDump` on both control processors, then contact EMC Customer Support Center.
For bladed switches, run `haDump` on both CP Cards.

Severity Information

HAMKERNEL-HTBT_DOWN

Message

```
<switch number> Info HAMKERNEL-HTBT_DOWN, 4, Heartbeat down
```

Explanation This message is logged when the active CP Card determines that the standby CP Card is down. This may happen as a result of an operator-initiated action, such as `firmwaredownload` or when the CP Card is reset or removed, or as a result of an error in the standby CP Card.

Action If no operator-initiated action has caused the error, then run `haDump` and `errDump` on the active CP Card. contact EMC Customer Support Center with the command outputs.

Severity Information

HAMKERNEL-HTBT_UP

Message

```
<switch number> Info HAMKERNEL-HTBT_UP, 4, Heartbeat up
```

Explanation This message is logged when the active CP Card detects the standby CP Card. This message indicates that the standby CP Card is available to take over in case a failure happens on the active CP Card. This message is typically seen when the standby CP Card reboots.

Action If no operator-initiated action has caused the error, then run `haDump` and `errDump` on the active CP Card. contact EMC Customer Support Center with the command outputs.

Severity Information

HAMKERNEL-WARNING

Message

```
<switch number> Info HAMKERNEL-WARNING, 4, <warning information>
```

Explanation This message is logged when a system warning has occurred. The *<warning information>* indicates where the problem is, and is used for troubleshooting.

Action Copy the error message, run the `hadump` and `errdump` command, and contact EMC Customer Support Center with the information. On an ED-12000B, obtain the output of `haDump` on both control processors.

For bladed switches, run the `hadump` command on both CP Cards.

Severity Information

21

HLO_System Error Messages

This chapter contains the following information:

Introduction

HLO is a part of FSPF protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.

HLO-DEADTIMEOUT

Message

```
<switch number> Error HLO-DEADTIMEOUT, 2, Incompatible Inactivity timeout
  <dead timeout> from port <port number>, correct value <value>
```

Explanation The HELLO message was incompatible. The dead timeout value does not match the value specified in the FSPF protocol. Since the dead timeout value is incompatible, the local switch will not accept FSPF frames from the remote switch.

Recommended Action The dead timeout value of the remote switch must be made compatible with the value specified in the FSPF protocol. See the manufacturer's documentation to change this value.

Severity Error

HLO-HLOTIMEOUT

Message

```
<switch number> Error HLO-HLOTIMEOUT, 2, Incompatible Hello timeout <HELLO
   timeout> from port <port number>, correct value <correct value>
```

Explanation The HELLO message was incompatible and timed out on the specified port. Since the HELLO timeout value is incompatible (the HELLO timeout value does not match the value specified in the FSPF protocol) the local switch will not accept FSPF frames from the remote switch.

Action The HELLO timeout value of the remote switch must be made compatible with the value specified in the FSPF protocol. See the manufacturer's documentation to change this value.

Severity Error

HLO-INVHLO

Message

```
<switch number> Error HLO-INVHLO, 2, Invalid Hello received from port <port
   number>, Domain = <domain ID>, Remote Port = <remote port ID>
```

Explanation The HELLO message received from the specified local port, domain ID, and remote port ID was reported to be invalid.

Action Since the HELLO message from the remote switch is incompatible with the local switch, the local switch will not accept FSPF frames from the remote switch. The HELLO message of the remote switch must be made compatible with the value specified in the FSPF protocol. See the manufacturer's documentation to change this value. Call Customer Support with questions.

Severity Error

22

kSWD_System Error Messages

This chapter contains the following information:

Introduction

The Kernel Software Watch Dog subsystem watches daemons for unexpected terminations and "hang" conditions, as well as informs the HAM module to take corrective actions such as failover or reboot. The numbers and values provided in each error message are data interpreted by engineering to analyze the cause of failure.

The following 21 applications are monitored by kSWD:

nsd	Name Server Daemon	zoned	Zone Daemon
emd	Environment Monitor	msd	Management Server Daemon
fabricd	Fabric Daemon	fspfd	FSPF Daemon
fcpd	FCPd Daemon	diagd	Diagnostics Daemon
snmpd	SNMP Daemon	track_changes	Track Changes Daemon
rpcd	FA-API RPC Daemon	evmd	EVM Daemon
psd	PS Daemon	rcsd	Reliable Commit Service Daemon
secd	Security Daemon	slapd	Slap Daemon
fwd	Fabric Watch Daemon	tsd	Time Service Daemon
webd	Web Tools Daemon	pdmd	PDM Daemon
fdmid	FDMI Daemon		

kSWD-APP_NOT_REFRESH_ERR

Message

```
<switch number> Critical kSWD-APP_NOT_REFRESH_ERR, 1, (k_SWD)Application
   with pid <number> not refreshing watchdog.
```

Explanation A critical kernel software error occurred in the Watch Dog subsystem. A kernel application is not able to refresh the watch dog. Refer to the specified PID number to find out which application is failing. The switch will reboot (on single-CP switches) or fail-over (on dual-CP switches).

Action Run the `savecore` command to find if a Core File was created. If a Core File is found, select the *FTP the file* option to send Core File(s) to customer support.

Copy the error message and contact customer support.

Severity Critical

kSWD-kSWD_GENERIC_ERR_CRITICAL

Message

```
<switch number> Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: <error
   message>
```

Explanation A critical application error was reported in the Watch Dog subsystem. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or fail-over (on dual-CP switches).

The error message may be any one of the following:

- <Detected unexpected termination of: <daemon name>>
  Explanation: One of the critical processes ended unexpectedly.
- <out of swdtab entries>
  Explanation: Internal resource limitation in the software watch dog table.
- <Performance error <number>>
  Explanation: Internal error.
- <<application name> failed to refresh SWD*** Sending SIGABRT to pid <process id number>>
  Explanation: One of the critical process applications is found to be non-responsive; Sending Signal Abort.
- <SWD: Reboot/Failover action
  Explanation: Software watch dog decided to reboot or failover the Control Processor (CP).
- <Sorry, registering the character device failed with <error number>>
  Explanation: Internal device registration error.
- <ERROR: can not set thresh secs wdt_period = <number>, savelog_thresh_period = <number>>
  Explanation: Internal setup/initialization error.
- <Error in unregister_chrdev: <number>>
  Explanation: Internal error.

Action Run the `savecore` command to find if a Core File was created. If a Core File is found, select the *FTP the file* option to send Core File(s) to customer support.

Copy the error message and contact customer support.

Severity Critical

23 LSDB_System Error Messages

This chapter contains the following information:

Introduction

Link State Database (LSDB) is a part of the FSPF protocol that manages the Link State Database.

LSDB-LSID

Message

```
<switch number> Error LSDB-LSID, 2, Link State ID <link state ID> out of
   range
```

Explanation The Link State Database ID is out of the acceptable range.

Action This record will be discarded and no user action is required.

Severity Error

LSDB-MAXINCARN

Message

```
<switch number> Info LSDB-MAXINCARN, 4, Local Link State Record reached max
   incarnation
```

Explanation The local Link State Database reached the maximum incarnations. An informational error message.

Action The incarnation number will wrap-around and no user action is required.

Severity Info

LSDB-NOLOCALENTRY

Message

```
<switch number> Critical LSDB-NOLOCALENTRY, 1, No database entry for local
  Link State Record,domain <local domain>
```

Explanation There is no local Link State Record entry in the Link State Database.

Action Perform a switch disable and enable.

Severity Critical

LSDB-NOLSR

Message

```
<switch number> Warning LSDB-NOLSR, 3, No Link State Record for domain
  <local domain>
```

Explanation There is no Link State Database record for the specified local domain.

Action Perform a switch disable and enable.

Severity Warning

24 MPATH_System Error Messages

This chapter contains the following information:

Introduction

Multicast Path (MPATH) uses the Shortest Path First (SPF) algorithm to dynamically compute a broadcast tree.

MPATH-NOPARENT

Message

```
<switch number> Error MPATH-NOPARENT, 2, Null parent, lsId = <number>
```

Explanation A null parent was reported. MPATH uses a tree structure in which the parent is used to connect to the root of the tree.

Recommended Action No user action required. Call Customer Support if error persists.

Severity Error

MPATH-NOPARENTLSR

Message

```
<switch number> Error MPATH-NOPARENTLSR, 2, Null lsrP, lsId = <ls ID number>
```

Explanation The Link State Record is null.

Action No action required.

Severity Error

MPATH-UNREACHABLE

Message

```
<switch number> Warning MPATH-UNREACHABLE, 3, No minimum cost path in
   candidate list
```

Explanation No minimum cost path (FSPF MPath) is available in the candidate list (the candidate list is customer defined).

Action No action required.

Severity Warning

25 MQ_System Error Messages

This chapter contains the following information:

Introduction

Message Queue (MQ) are used for inter-process communication. Message queues allow many messages, each of variable length, to be queued.

- Any process or Interrupt Service Routine (ISR) can write messages to a message queue.
- Any process can read messages from a message queue.

MQ-MSGTYPE

Message

```
<switch number> Error MQ-MSGTYPE, 2, mqRead, queue = <queue name>, queue ID
  = <queue ID> type = <message type>
```

Explanation An unexpected message has been received in the specified message queue. The message queue name and the type of the message are indicated in message.

The following variables may be displayed in the error message:

- *<queue name>*
  fspf_q
- *<queue ID> <message type>*
  2MSG_TX
  3MSG_INTR
  4MSG_STR
  6MSG_ASYNC_IU
  7MSG_LINIT_IU
  8MSG_RSCN
  9MSG_IOCTL
  10MSG_ACCEPT
  11MSG_IU_FREE
  12MSG_US
  13MSG_EXT_RSCN
  14MSG_RDTS_START
  15MSG_RDTS_SENDEFP
  16MSG_RDTS_RESET

Recommended Action Run the `mqshowall` command and record the output. Provide the `mqshowall` output as well as the error message, and contact EMC Customer Support Center.

Severity Error

26

MS_System Error Messages

This chapter contains the following information:

Introduction

The Management Service allows the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas:

- **Fabric Configuration Server** - provides for the configuration management of the fabric
- **Unzoned Name Server** - provides access to Name Server information that is not subject to Zone constraints.
- **Fabric Zone Server** - provides access to and control of Zone information

MS-INVALID_CTRESP

Message

```
<switch number> Error MS-INVALID_CTRESP, 2, MS Invalid CT Response from
   <domain>
```

Explanation The Management Server (MS) received an invalid Common Transport (CT) response from *<domain>*. The MS expects either a CT accept IU or a reject IU; the management server received neither response, which violates the FS-GS spec.

Action Check the integrity of the interconnect element at the specified domain.

Severity Error

MS-OUT_RESOURCES

Message

```
<switch number> Error MS-OUT_RESOURCES, 2, MS Failure while initializing
   <action>
```

Explanation The Management Server (MS) failed while initializing the specified *<action>*.

The following *<actions>* may be displayed:

- *<while writing to ms_els_q>*
  Explanation: Unable to write a message to the Management Server Extended Link Service Queue.
- *<while inserting timer to timer list>*
  Explanation: Unable to add timer to resource.

Action The switch may be temporarily busy and out of resources to respond to a request. If the error happens frequently, check the available memory on the switch using **memshow** and contact EMC Customer Support Center.

Severity Error

MS-PLDBSEG

Message

```
<switch number> Warning MS-PLDBSEG, 3, MS Platform Segmented port=<port
  number> (<reason for segmentation> D= <domain>)
```

Explanation The Management Server (MS) has segmented from another switch <*domain*> at the specified <*port number*> due to errors or inconsistencies defined in the MS Platform Service.

The following <*reasons for segmentation*> may be displayed:

- <EXGPLDB failed: Unable to Activate Platform>
  Explanation: Exchange of Platform Service database between fabrics has failed because activation of MS Platform Services failed on the other switch.
  Action: The other switch may not support MS Platform Service. Check capability using **mscapabilityshow**.

- <PLCOMIT failed: Unable to activate Platform>
  Explanation: Exchange of Platform Service database between fabrics has failed due to the failure of conditional activation of MS Platform Services on the other switch.
  Action: contact EMC Customer Support Center.

- <EXGPLDB failed: Platform DB not mergeable>
  Explanation: Exchange of Platform Service database between fabrics has failed due to conflicting databases between the switches.
  Action: Ensure mergeability of connecting fabrics. For example, some DB objects may have conflicting definitions. Use **msplatshow** to show content of DB and check for conflicts.

- <EXGPLDB failed: DB size exceeds limit>
  Explanation: Exchange of Platform Service database between fabrics has failed due to the violation of size allowance for MS Platform database.
  Action: Ensure that the merged databases will not have a final database size that exceeds the MS Platform database size limitation of 32K.

- *<Timeout: Ran out of retry count>*
  Explanation: Exceeded number of tries to merge MS Platform database with another fabric. Errors may be present in the fabric intercommunication.
  Action: Check cable and logical link to ensure healthy and retry fabric merge. If error recurs, contact EMC Customer Support Center.

- *<Security: security conflict>*
  Explanation: Security is currently enforced and configuration state of MS Platform Service between merging fabrics is inconsistent.
  Action: Fabric may have enabled and disabled MS Platform Service states. make both fabrics consistent using the commands **msplmgmtactivate** and **msplmgmtdeactivate**.

Action See individual *<reasons for segmentation>* in Explanation above.

Severity Warning

MS-PLSTATE

Message

```
<switch number> Debug MS-PLSTATE, 5, MS Platform Service Unstable(<function
   code>: <message string> D= <domain number>)
```

Explanation The management server (MS) Platform Service is unstable.

The following variables may be displayed:

- *<function code>* invoking error
  - *<capmat>* - msPlCapMatrix
  - *<CA>* - msPlCondActivate
- <message string>
  - *<No Resp for GCAP from>*
    Explanation: Switch did not respond to a request for GCAP (MS Get Capabilities) command.
    Action: No user action required.
  - *<GCAP sup but not PL by>*
    Explanation: GCAP (MS Get Capabilities) is supported but the flag for MS Platform Service is not set. Inconsistency observed.
    Action: Set the flag for the MS Platform Service.
  - *<GCAP Rejected (reason =BUSY) by>*
    Explanation: GCAP (MS Get Capabilities) is not supported by another switch.
    Action: No action required.
  - *<Reject EXGPLDB from>*
    Explanation: Request to exchange platform database was rejected. Other switch may be busy.
    Action: No action required.
- *<domain number>*
  Explanation: Target domain that caused error. Unique to fabric.

Action See individual *<message string>* in Explanation above.

Severity Debug

MS-RCSFAILED

Message

```
<switch number> Debug MS-RCSFAILED, 3, MS RCS failed. MS CT command = <CT
   command> RCS reason =<RCS reason code> (<RCS reason code string>)
```

Explanation Usage of the Reliable Commit Service (RCS) has failed in MS.

The specified MS <*Command Transport command* > for an RCS request failed for the specified <*RCS reason*> and is described in more detail in the <*RCS reason code string*>.

Action Copy error message information and contact EMC Customer Support Center.

Severity Debug

MS-TIME_OUT

Message

```
<switch number> Error MS-TIME_OUT, 2, MS time out while <error>
```

Explanation The Management Server (MS) timed out while acquiring a resource.

The following is displayed as the <*error*>:

- <*acquiring elsSemaRNID lock*>
  Explanation: Unable to acquire a semaphore lock for Request Node Identification Data (RNID).

Action Reboot switch and retry request. If error recurs, contact EMC Customer Support Center.

Severity Error

MS-UNEXPECTED_IUDATASZ

Message

```
<switch number> Error MS-UNEXPECTED_IUDATASZ, 2, MS Unexpected iu_data_sz=
   <number of bytes>
```

Explanation The Management Server (MS) received IU data of unexpected size. The IU payload and the IU size may be inconsistent with each other or with the command that is currently being processed.

Action Retry operation. If error recurs, contact EMC Customer Support Center.

Severity Error

MS-UNSTABLE_DCOUNT

Message

```
<switch number> Debug MS-UNSTABLE_DCOUNT, 5, MS detected ONLY 1 Domain
   <domain in local resource>.
```

Explanation The Management Server (MS) detected an unstable count of domains in its own local resource.

Action The fabric may be unstable. Try operation again later or contact EMC Customer Support Center.

Severity Debug

MS-UNSTABLE_FABRIC

Message

```
<switch number> Debug MS-UNSTABLE_FABRIC, 5, MS detected Unstable
   Fabric(function code>: <message string> d= <domain number>).
```

Explanation The Management Server (MS) detected an unstable fabric; the command or operation may not be successfully completed.

- *<function code>* invoking error
  - *<MsgPlatDBProc>* - msPlatMsgPlatDBProc
  - *<MsgGCAP>* - msPlatMsgGCAP
  - *<MsgPl(D)ACTV> - MsPlayMsgActivateProc*
- <message string>
  - *<DOMAIN_INVALID for a req from>*
    Explanation: Domain is invalid for a request.
  - *<No WWN for>*
    Explanation: Unable to acquire the World Wide Name (WWN) for corresponding domain.
- *<domain number>*
  Explanation: Target domain that caused error. Unique to fabric.

Action Copy error message string and contact EMC Customer Support Center.

Severity Debug

27 NBFSM_System Error Messages

This chapter contains the following information:

Introduction

NBFSM is a part of the FSPF (Fabric Shortest Path First) protocol that handles a neighboring or adjacent switches' Finite State Machine.

Input to FSM is an event and is used to move a neighboring or adjacent (directly connected to the local switch) switch from one state to another based on specific events. For example, when two switches are connected to each other using an ISL (interswitch link) cable, they will be in Init State. After both switches receive HELLO messages, they move to the Database Exchange State and so on.

NBFSM states are: Down (0), Init(1), Database Exchange (2), Database Acknowledge Wait(3), Database Wait (4), Full (5).

NBFSM-DUPEPORTSCN

Message

```
<switch number> Debug NBFSM-DUPEPORTSCN, 5, Duplicate E_Port SCN from port
  <port number> in state <state change number>
```

Explanation A duplicate E_Port State Change Number was reported.

Recommended Action No action required.

Severity Debug

NBFSM-NGBRSTATE

Message

```
<switch number> Error NBFSM-NGBRSTATE, 2, Wrong input: <state name> to
   neighbor FSM, state <current state name>, port <number>
```

Explanation The wrong input was sent to the neighbor Finite State Machine.

Action The input will be discarded and no user action is required.

Severity Error

NBFSM-XMITFLAG

Message

```
<switch number> Warning NBFSM-XMITFLAG, 3, DB_XMIT_SET flag not set in state
   <current state name> input <state name>, port <number>
```

Explanation From the current state, the Data Base transmit set flag was not set for the specified input state on the specified port.

Action No user action required.

Severity Warning

28

PANIC_System Error Messages

This chapter contains the following information:

Introduction

Panic errors are a result of unexpected software-related conditions.

PANIC-INCONSISTENT

Message

```
<switch number> Panic PANIC-INCONSISTENT, 0, <panic message>
```

Explanation The Name Server module is trying to sort data and discovers that the expected number of entries does not match the actual number of entries found. The *<panic message>* provides unique information for troubleshooting.

Action Copy the error message and contact customer support.

Severity Panic

PANIC-LSDB_CKSUM

Message

```
<switch number> Panic PANIC-LSDB_CKSUM, 0, Link State Database checksum
   failed, lsdbeP = <hexadecimal number>, lsrP = <hexadecimal number>, LSID
   = <decimal number>
```

Explanation Error verifying the checksum in the Link State Database. This error message is used in the FSPF (Fabric Shortest Path First) module. The additional information provided includes:
lsdbeP: Link State Database Element Pointer
lsrP: Link State Record Pointer
LSID: Link State Identifier

Action Copy the error message and contact EMC Customer Support Center.

Severity Panic

PANIC-MALLOC

Message

```
<switch number> Panic PANIC-MALLOC, 0, malloc failed <additional
   information>
```

Explanation Error message shows a memory allocation failed, and provides *<additional information>*.

Action Copy the error message and call EMC Customer Support Center.

Severity Panic

PANIC-QCREATE

Message

```
<switch number> Panic PANIC-QCREATE, 0, mqCreate failed
```

Explanation Failed to create a message queue. Further details about this error are printed on the console.

Action Copy console output, run `supportshow`, and contact EMC Customer Support Center.

Severity Panic

PANIC-SEMCREATE

Message

```
<switch number> Panic PANIC-SEMCREATE, 0, semCreate failed
```

Explanation The Reliable Commit Service (RCS) subsystem used for Security, Mgmt Service, and Zoning, failed to create a semaphore.

Action Run `supportshow` and contact EMC Customer Support Center.

Severity Panic

29 PDM_System Error Messages

This chapter contains the following information:

Introduction

Parity Data Manager (PDM) is a user space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition, and from the active CP Card to the standby CP Card.

PDM-CONFIG

Message

```
<switch number> Warning PDM-CONFIG, 3, Failed to parse pdm config
```

Explanation PDM process could not parse the config file. This may be caused by missing config file during the installation.

Action Re-install firmware. If error recurs, contact EMC Customer Support Center.

Severity Warning

PDM-FCREATE

Message

```
<switch number> Warning PDM-FCREATE, 3, File not created: <file name>
```

Explanation PDM failed to create *<file name>*.

Action contact EMC Customer Support Center.

Severity Warning

PDM-FOPEN

Message

```
<switch number> Warning PDM-FOPEN, 3, File open failed: <file name>
```

Explanation PDM could not open <*file name*>.

Action contact EMC Customer Support Center.

Severity Warning

PDM-FREAD

Message

```
<switch number> Warning PDM-FREAD, 3, File read failed: <file name>
```

Explanation PDM could not read data from <*file name*>.

Action contact EMC Customer Support Center.

Severity Warning

PDM-FWRITE

Message

```
<switch number> Warning PDM-FWRITE, 3, File write failed: <file name>
```

Explanation PDM could not write data to <*file name*>.

Action contact EMC Customer Support Center.

Severity Warning

PDM-WWNFAIL

Message

```
<switch number> Warning PDM-WWNFAIL, 3, Unable to write gen to WWN: <error
   code>
```

Explanation PDM failed to write generation number to the WWN Card.

Action Copy error code and contact EMC Customer Support Center.

Severity Warning

30 PLATFORM_System Error Messages

This chapter contains the following information:

Introduction

Platform (Service) Errors come from the port blade and CP blade. These error messages indicate any problems for each of these two hardware components, including problems coming from the PCI buses, i2c bus, FPGA (Field Programmable Gate Array), and power.

PLATFORM-CPLD_CTRL

Message

```
<switch number> Warning PLATFORM-CPLD_CTRL, 3, <specific error message>
```

Explanation The diagnostic software failed to set the FC clock. The firmware is likely corrupted.

The following messages may be displayed in the *<specific error message>*:

- fabsys_get_hwStatus: invalid H/W unit
  Explanation: The system is trying to get hardware status on a specific blade in a specific slot, but the reported information is not valid.
- fabsys_set_hwUnit: invalid H/W unit
  Explanation: The system is trying to set the status of a blade in a specific slot, but the corresponding data is not valid.
- Can't release i2c bus: copy_from_user failed
  Explanation: The system cannot copy data from userspace to kernel, so i2c bus cannot be released.
- Can't access FC clock: get_user_ failed
  Explanation: The system cannot get data from the userspace to kernel, so cannot access the FC clock on the port blade.
- Can't get FC clock: put_user failed
  Explanation: The system cannot put the data from kernel to userspace, so access to FC clock failed.

Recommended Action Download new firmware and reboot.

Severity Warning

PLATFORM-FUNCT_FAIL

Message

```
<switch number> Critical PLATFORM-FUNCT_FAIL, 1, <specific error message>
```

Explanation The i2c bus has a problem that cannot be fixed by the system driver. This error is periodically followed by another error on a particular hardware unit connected to that bus.

The following messages may be displayed in the *<specific error message>*:

- sysCfgSelectMaster Failed
  Explanation: System failed to select HA master.
- sysHaInit can't initialize HA
  Explanation: HA failed to be initialized.
- fabsys_set_cpMaster Select/Set CP master failed
  Explanation: The system failed to select or set the HA CP master.
- fabsys_set_cpMaster Set mastership failed
  Explanation: The system failed to select or set the HA CP master.
- fabsys_set_ownSwMask Set own-switch mask failed
  Explanation: The system failed to set up switch mask. The switch mask is bitmap which corresponds to the switch number.

Action Try unplugging and replugging in the CP card. If this doesn't work, try cycling the power for the switch. If these don't work, re-install the firmware.

Severity Critical

PLATFORM-MALLOC

Message

```
<switch number> Critical PLATFORM-MALLOC, 1, <specific error message>
```

Explanation The memory allocation failed. The system is low on memory, has severe memory fragmentation, or has a memory leak. The following message will be displayed in the *<specific error message>*: < pciInitBlade Allocate memory for new blade failed>.

Action Reboot the switch. If the problem is not resolved, update the firmware.

Severity Critical

PLATFORM-NOT_SUPPORT (Critical)

Message

```
<switch number> Critical PLATFORM-NOT_SUPPORT, 1, <error message> (<name>=
  <value>)
```

Explanation The specified platform is not supported or the firmware is corrupt.

Action Check the FRU header of the blade (if the blade ID is supported); download new firmware and reboot.

Severity Critical

PLATFORM-NOT_SUPPORT (Warning)

Message

```
<switch number> Warning PLATFORM-NOT_SUPPORT, 1, <error message>
```

Explanation The specified platform is not supported or the firmware is corrupt.

Action Check the FRU header of the blade (if the blade ID is supported); download new firmware and reboot.

Severity Warning

PLATFORM-NULL_VAL

Message

```
<switch number> Critical PLATFORM-NULL_VAL, 1, <null value>
```

Explanation A null pointer is detected.

Action No action required.

Severity Critical

PLATFORM-SERVICE

Message

```
<switch number> Warning PLATFORM-SERVICE, 3, <specified message reason>
```

Explanation The specified platform failed for the reason displayed in the message. Some application failed to use the system driver. The firmware is likely corrupt.

Action Download new firmware and reboot.

Severity Warning

PLATFORM-SYSPCI_CFG

Message

```
<switch number> Critical PLATFORM-SYSPCI_CFG, 1, <function name> <specified
   error message>
```

Explanation System Driver failed to initialize the CP board (specifically the PCI bridges on the CP). There is likely a hardware problem on the CP board; the bridges may be damaged.

Action Cycle power on the CP Card. If this doesn't correct the problem, replace the CP Card.

Severity Critical

31

PORT_System Error Messages

This chapter contains the following informtion:

Introduction

These PORT error messages deal with the front-end user ports on the switch. Front-end user ports are directly accessible by users to connect end devices or connect to other switches.

PORT-ENABLE_FAIL

Message

```
<switch number> Info PORT-ENABLE_FAIL, 4, Port <port number> could not be
   enabled because it is disabled due to long distance.
```

Explanation The specified port could not be enabled because other ports in the same quad have used up the buffers available for this quad. This happens when other ports were configured to be long distance.

Recommended Action To enable this port, the user can reconfigure the other E_ports so they are "not long distance", or the user can change the other E_ports so they are not E_ports. This will free up some buffers and allow this port to be enabled.

Severity Info

PORT-LINK_FAULT

Message

```
<switch number> Warning PORT-LINK_FAULT, 3, Port <port number> Faulted
   because of many Link Failures
```

Explanation The specified port is now disabled because the link on this port had multiple failures within a short amount of time. This problem is typically related to hardware.

Action Check and replace (if necessary) the hardware attached to both ends of the specified *<port number>*, including:

- the media (GBICs/SFPs),
- the cable (fibre optic or copper ISL), and
- the attached devices.

When finished checking the hardware, perform `portenable` to re-enable the port.

Severity Warning

32 PS_System Error Messages

This chapter contains the following information:

Introduction

The Performance Server daemon measures the amount of traffic between end points, or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.

PS-ASPINIT

Message

```
<switch number> Error PS-ASPINIT, 2, PS: <name of function>(): aspInit()
  failed.
```

Explanation The Application Service Provide (the ASP library for all daemons) failed to initialize. The *<name of function>* provides the specific area that this ASPINIT failure occurred; this failure only occurs in the "main()" portion of the Performance Server daemon.

Action Copy the error message, run `supportshow` and call EMC Customer Support Center.

Severity Error

PS-ASSERT

Message

```
<switch number> Error PS-ASSERT, 2, ASSERT <#> PS: Assertion failed <expr>
  <file>:<line> Function: <function>() <argument1> <argument2> <argument3>
```

Explanation The software assertion failed. The<#> is the number of arguments in the assertion, *<expr>* is the expression causing the assertion, *<file>* is the file name, <line> is the line number, and *<function>* is the function name. The *<arguments 1,2,3>* provide additional information about this assertion.

Action Run the `supportshow` command, copy the error message output and send both pieces of information to EMC Customer Support Center.

Severity Error

PS-CALLOC

Message

```
<switch number> Error PS-CALLOC, 2, PS:<name of function>() Failed to
  allocate <number of bytes> bytes
```

Explanation The switch failed to allocate the specified number of bytes of memory for the specified *<name of function>*. The function area is specified in the error message; this error can occur in any area in which memory is allocated.

Action Run the `supportshow` command for further information regarding memory allocation. Copy the error message and contact customer support.

Severity Error

PS-HAINIT

Message

```
<switch number> Error PS-HAINIT, 2, PS: <name of function>(): ps_init_ha()
   failed.
```

Explanation The Hi-Availability initiation failed. The function area is specified in the error message; this error only occurs in "ps_init()".

Action Copy the error message and contact customer support.

Severity Error

PS-IPCINIT

Message

```
<switch number> Error PS-IPCINIT, 2, PS: <name of function>(): ipcInit()
   failed.
```

Explanation The performance monitor Inter Process Communication (IPC) initiation failed. The IPC is the method used by the switch to communicate with all daemons. The function area is specified in the error message; this error only occurs in "main()".

Action Run the `supportshow` command and contact customer support.

Severity Error

PS-IPCEXIT

Message

```
<switch number> Error PS-IPCEXIT, 2, PS: <name of function>(): ipcInit()
   failed.
```

Explanation The Inter Process Communication (IPC) failed to exit. The IPC is the method used by the switch to communicate with all daemons. The function area is specified in the error message; this error only occurs in "main()".

Action Copy the error message and contact customer support.

Severity Error

PS-MALLOC

Message

```
<switch number> Error PS-MALLOC, 2, malloc failed <argument 1 >
```

Explanation The switch failed memory allocation. The information provided in *<argument 1>*describes where in the code the error occurred, for engineering troubleshooting.

Action Run the `supportshow` command for further information regarding memory allocation. Copy the output and the error message and send both pieces of information to EMC Customer Support Center.

Severity Error

PS-TASKCREATE

Message

```
<switch number> Error PS-TASKCREATE , 2, PS: taskCreate() failed to create
  task <argument 1>
```

Explanation The Performance Server daemon failed to create a PSD task. The *<argument1>* provides details about this failure.

Action Run the `supportshow` command and contact customer support.

Severity Error

PS-THRCREATE

Message

```
<switch number> Error PS-THRCREATE, 2, PS: <name of function>():
  pthread_create() failed to create <name of thread>, rc = <return code>
```

Explanation The PS thread was not created due to an unknown reason; a resource allocation problem may be the cause. The function area is specified in the error message; this error only occurs in ps_init() and ps_reqmgr_init().

The possible return codes (RC) are:

- EAGAIN (-11)
- EINVAL (-22)
- EPERM (-1)

Action Run the `supportshow` command for further information regarding memory allocation. Copy the error message and contact customer support.

Severity Error

33 RAPID_System Error Messages

This chapter contains the following information:

Introduction

The Remote API Daemon (RAPID) is used by the Fabric Access for API-related tasks.

RAPID-AUTH_ERR

Message

```
<switch number> Warning RAPID-AUTH_ERR, 3, Authentication Error: client <IP
  address> has bad credentials: <bad user name and password pair>
```

Explanation An authentication error was reported. The specified <*client IP address*> has bad credentials.

Action Enter correct root, admin, or user name and password pair from the Fabric Access API host.

Severity Warning

34 RCS_System Error Messages

This chapter contains the following information:

Introduction

Reliable Commit Service (RCS) Error Messages gets a request from Zoning, Security, or Management Server for passing data messages to switches in the fabric. RCS then asks RTWR to deliver the message. RCS also acts as a gatekeeper, and limits the number of outstanding requests per Zoning, Security, or Management Server module.

RCS-RCSDISABLED

Message

```
<switch number> Debug RCS-RCSDISABLED, 5, RCS has been disabled. Some
   switches in the fabric do not support this feature
```

Explanation The RCS feature has been disabled on the local switch because not all switches in the fabric support RCS. Currently 2.6, 3.1, and 4.1 support the RCS feature.

Recommended Action Upgrade firmware to support RCS.

Severity Debug

RCS-RCSENABLED

Message

```
<switch number> Debug RCS-RCSENABLED, 5, RCS has been enabled.
```

Explanation The RCS feature has been enabled.

Action None required.

Severity Debug

RCS-RCSENOMEM

Message

```
<switch number> Error RCS-RCSENOMEM, 2, Failed to allocate memory: <function
   name>
```

Explanation Error: No Memory. The specified RCS function failed to allocate memory.

Action Check memory usage on the switch. Collect *<function name>* information provided in the message and call EMC Customer Support Center.

Severity Error

RCS-APP_NOTREG

Message

```
<switch number> Error RCS-APP_NOTREG, 0, Application <application name> not
   registered, HA State Replication ineffective
```

Explanation If the specified application does not register with RCS, then RCS returns this error.

Action Collect *<application name>* information provided in the message and call EMC Customer Support Center.

Severity Error

RCS-LOCAL_REJECT

Message

```
<switch number> Information RCS-LOCAL_REJECT, 1, State <current state>,
   Application <application ID> returned <reject reason>
```

Explanation The specified application on another switch rejects this RCS transaction with the specified reject reason, then RCS returns this error and RCS aborts the current transaction. The current state describes at what point in the transaction the reject occurred.

Action For the first reject, wait until the other user finishes, then re-send transaction. If this reject happens again, examine correctness of the data being passed. If the data is correct, collect information provided in the error message and call EMC Customer Support Center.

Severity Information

35 RPCD_System Error Messages

This chapter contains the following information:

Introduction

The Remote Procedure Call Daemon is used by the Fabric Access for API-related tasks.

RPCD-AUTH_ERR

Message

```
<switch number> Warning RPCD-AUTH_ERR, 3, Authentication Error: client <IP
  address> has bad credentials: <bad user name and password pair>
```

Explanation An authentication error was reported. The specified *<client IP address>* has bad credentials.

Action Enter correct root, admin, or user name and password pair from the Fabric Access API host.

Severity Warning

RPCD-INIT_FAIL

Message

```
<switch number> Error RPCD-INIT_FAIL, 2, Initialization Error: <function>
   failed, error code = <error code number>
```

Explanation The RPCD initialization failed due to the specified reason.

The following variables may be displayed:

- <function>
  - *<apigetsysconfig>*
    Explanation: Provides the daemon information about the number of switches in the chassis and which is the master.
  - <socket>
    Explanation: Method to initialize TCP/IP communication between host and switch.
  - <bind>
    Explanation: Method to initialize TCP/IP communication between host and switch.
  - *<svctcpcreate>*
    Explanation: Method to initialize RPC interface between host and switch.
  - *<scv_register>*
    Explanation: Method to initialize RPC interface between host and switch.
  - *<pthread_create>*
    Explanation: Method to initialize FSS thread.
- <error code number>
  - -1 = failed

Action Re-install Fabric OS firmware and reboot. If the error recurs, copy error message and contact EMC Customer Support Center.

Severity Error

36

RTWR_System Error Messages

This chapter contains the following information:

Introduction

Reliable Transport Write and Read (RTWR) helps deliver data messages to specific switches in the fabric or all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, then RTWR would return an "unreachable" message to the caller, allowing the caller to take the appropriate action. If a switch is not responding then RTWR would re-try 100 times.

RTWR-FAILED

Message

```
<switch number> Error RTWR-FAILED, 2, RTWR <routine: error message>, <detail
   1>, <detail 2>, <detail 3>, <detail 4>, <detail 5>
```

Explanation The RTWR failed. The *<routine: error message>* provides the name of the routine having the error, and, if displayed, specific error information is provided after the colon. Additionally, *<details 1 2 3 4 5>* provide details to help the user or EMC Customer Support isolate the problem.

The error message may display any of the following details:

- "rtwrInit: No Memory", 0x9abc, 0x8def, 100, 50, 123
  Explanation: RTWR has run out of memory inside the rtwrInit function.
  <Detail 1>, if non-zero, contains the pointer of the payload received.
  <Detail 2>, if non-zero, contains the switch ID of the destination domain.
  <Detail 3>, if non-zero, contains the size of memory we want to allocate.
  <Detail 4>, if non-zero, contains the thread ID.
  <Detail 5>, if non-zero, contains the process ID.
  Action: Check the memory usage on the switch.
- "rtwrTask: mqRead failed", 0, 0, 0, 0, 0
  Explanation: Cannot read from a message queue. May be out of memory.
  Action: Check the memory usage on the switch or call EMC Customer Support .

- "rtwrTask exited unexpectedly", 0, 0, 0, 0, 0
  Explanation: Internal error
  Action: Call EMC Customer Support
- 'rtwrRequest: No memory", 0, 0, 0, 0, 0
  Explanation: RTWR has run out of memory inside the rtwrInit function.
  <*Detail 1*>, if non-zero, contains the pointer of the payload received.
  <*Detail 2*>, if non-zero, contains the switch ID of the destination domain.
  <*Detail 3*>, if non-zero, contains the size of memory we want to allocate.
  <*Detail 4*>, if non-zero, contains the thread ID.
  <*Detail 5*>, if non-zero, contains the process ID.
  Action: Check the memory usage on the switch.
- "rtwrAsyncMultiRequest", 0, 0, 0, 0, 0
  Explanation: Internal error.
  Action: Call EMC Customer Support .
- "rtwrAsyncMultiRequest: pidlist_copy failed", 0, 0, 0, 0, 0
  Explanation: Out of memory.
  Action: Check the memory usage on the switch or call EMC Customer Support .
- "rtwrSyncRequest" , 0, 0, 0, 0, 0
  Explanation: Internal error.
  Action: Call EMC Customer Support .
- "rtwrSyncRequest: Unreachable domain", 0xff, domain, 0x9abc, domain, 0xff
  Explanation: Domain is notreachable.
  Action: Use `fabricshow` to see if domain is offline. Check the physical ISLs for the domain.
- "rtwrSyncRequest: Cannot create sync. semaphore", 0, 0, 0, 0, 0
  Explanation: Out of memory.
  Action: Check the memory usage on the switch or call EMC Customer Support .
- "rtwrSyncRequest: Cannot write message queue", 0, 0, 0, 0, 0
  Explanation: Out of memory.
  Action: Check the memory usage on the switch or call EMC Customer Support .

- "rtwrSyncRequest: semaTake failed", 0, 0, 0, 0, 0
  Explanation: Internal error.
  Action: Call EMC Customer Support .
- "rtwrMsgProcess: msg NULL", 0, 0, 0, 0, 0
  Explanation: An empty message has been received. Internal error.
  Action: Call EMC Customer Support .
- "rtwrRequestProcess: target_bm Null", 0, 0, 0, 0, 0
  Explanation: Out of memory.
  Action: Check the memory usage on the switch or call EMC Customer Support
- "rtwrRequestProcess: cannot allocate fcAsyncMultiCB_t", 0, 0, 0, 0, 0
  Explanation: Out of memory.
  Action: Check the memory usage on the switch or call EMC Customer Support .
- "rtwrRequestProcess: rtwrMultiTransmit failed", 0, 0, 0, 0, 0
  Explanation: Transmission of payload to multiple destinations failed.
  Action: Call EMC Customer Support.
- "rtwrRespProcess", 0, 0, 0xff, 0xff, 0xff
  Explanation: Invalid pointer to payload.
  Action: Call EMC Customer Support.
- "rtwrRespProcess", ...
  Explanation: Internal error.
  Action: Call EMC Customer Support.
- "rtwrRespProcess: release_kiu failed", ..., 0,0
  Explanation: Internal error.
  Action: Call EMC Customer Support.
- "rtwrRespProcess: no such state", 0, 0, 0, 0, 0
  Explanation: Internal error.
  Action: Call EMC Customer Support.
- "rtwrTransmit", domain, ...
  Explanation: Transmission problem to specified domain.
  Action: Use `fabricshow` to see if domain is offline. Check the physical ISLs for the domain. Call EMC Customer Support.
- "rtwrTransmit: fcAsyncMultiSend failed", 0, 0, 0, 0, 0
  Explanation: Internal error.
  Action: Call EMC Customer Support.

Action See action provided with each appropriate message above.

Severity Error

RTWR-TRANSMIT

Message

```
<switch number> WARNING RTWR-TRANSMIT, 3, RTWR <error message>, <detail1>,
   <detail2>, <detail3>, <detail4>, <detail5>
```

Explanation RTWR has exhausted the maximum number of retries sending data to the specified domain. Details are as follows:

- *<error message>:* RTWRTransmit: Maxretries exhausted
- *<detail1>*: Port
- *<detail2>*: Domain
- *<detail3>*: Retry Count
- <detail1>: Status
- *<detail1>* Process ID

Action User should check whether specified Domain ID is offline. Use fabricshow to see if the specified Domain ID is online. Call EMC Customer Support if error persists.

Severity Warning

37 SCN_System Error Messages

This chapter contains the following information:

Introduction

The internal State Change Notification is used for state change notifications from the kernel to the daemons within FabOS.

SCN-SCNQ_OVERFLOW

Message

```
<switch number> Critical SCN-SCNQ_OVERFLOW, 1, SCN queue overflow for
  <daemon name>
```

Explanation An attempt to write a State Change Notification message to a specific SCN queue has failed because the SCN queue for the specified *<daemon name>* is full. This may be caused by the daemon "hanging", or if the system is busy.

The variables for the *<daemon name>* are:
fabricd
asd
evmd
fcpd
webd
msd
nsd
psd
snmpd
zoned
fspfd
tsd

Recommended Action If this is caused by a "hung" daemon, eventually the software watchdog will kick in and cause the daemon to core dump. Save the console messages and the core dump and contact EMC Customer Support Center. If the system is busy, the condition will be temporary.

Severity Critical

38 SEC_System Error Messages

This chapter contains the following information:

Introduction

This section describes security errors, warnings, or information that happens during secure-related data management or fabric merge in secure mode. Administrators should pay more attention on secure fabric to distinguish between internal switch/fabric operation error or external attack. In case of external attack, administrator should react properly to stop the attack and protect the fabric securely.

SEC-RSENDFAIL

Message

```
<switch number> Error SEC-RSENDFAIL, 2, RCS process fails: %s
```

Explanation The RCS (reliable commit service) process fails to complete. RCS is a reliable mechanism to transfer data from one switch to the other switches within the fabric. This mechanism guarantees that either all switches commit to the new database or none of them update to the new database. This process can fail is one switch in the fabric is busy or in an error state that can not accept the database.

Recommended Action RCS is used when the security database is changed by a command issued by security (e.g., secPolicySave, secPolicyActivate, secVersionReset...). If the switch is busy, the command might fail the first time only. Retry after first fail. If the command fails consistently, contact EMC Customer Support Center.

Severity Error

SEC-SECDBFAIL

Message

```
<switch number> Warning SEC-SECDBFAIL, 3, Security data fails: %s
```

Explanation This message occurs when the receiving switch fails to validate the security database sending from the primary FCS switch. Probable causes for this error can be: the data package is corrupted, the time stamp on the package is out of range as a result of replay attack or out of sync time service or the signature verification failed. Signature verification failure may be due to a internal error such as losing the primary public key or may be due to an invalid database.

Action Issue secFabricShow command to verify the fabric is still consistent. All the switches should be in READY state. If a switch is in Error state, the database may not be correctly updated for that specific switch. Follow standard recovery process. The error may also be a result of an internal corruption or a hacker attack to the secure fabric.

Severity Warning

SEC-SECDLFAIL

Message

```
<switch number> Warning SEC-SECDLFAIL, 3, Fail to download security data to
   domain <domain number> after <number of retries> retries
```

Explanation The specified domain number failed to download security data after the specified number of attempts. The primary will segment the failure switch after 30 tries. The failure switch may have some internal error and failed to accept the database download.

Action Reset the version stamp on the switch to 0 then rejoin the switch to the fabric. If the switch consistently fails, contact EMC Customer Support Center.

Severity Error

SEC-SECINFO

Message

```
<switch number> Info SEC-SECINFO, 4, %s
```

Explanation The switch may exhibit low memory, queue full, fail to set password or fail to set SNMP string.

Action Depending on the information message, it is recommended to check the status of the switch then retry the process or command. If the problem persists, contact EMC Customer Support Center.

Severity Info

SEC-SECINFORM

Message

```
<switch number> Info SEC-SECINFORM, 4, Primary FCS receives data request
   from domain <domain number>
```

Explanation The primary FCS received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection) a message is generated to the primary FCS to try to correct and re-sync with the rest of the switches in the fabric.

Action Check the fabric status using secFabricShow to verify the fabric is not being attacked by unauthorized users.

Severity Info

SEC-SEC_STATS

Message

```
<switch number> Warning SEC-SEC_STATS, 3, Security statistics error: %s
```

Explanation Logs each error for any statistic related command for security (secStatsShow, secStatsReset) to keep track of any security violations on the switch. The counter is updated automatically when a security violation occurs. This message may also occur if the updating counter fails.

Action If the message is the result of a user command, retry the statistic command. If the problem persists, contact EMC Customer Support Center.

Severity Warning

SEC-SECVIOL_API

Message

```
<switch number> Info SEC-SECVIOL_API, 4, Security violation: Unauthorized
  host with IP address <IP address> tries to establish API connection.
```

Explanation A security violation was reported. The specified unauthorized host attempted to establish an API connection.

Action Check for any unauthorized access to the host via the switch through the API connection.

Severity Info

SEC-SECVIOL_HTTP

Message

```
<switch number> Info SEC-SECVIOL_HTTP, 4, Security violation: Unauthorized
  host with IP address <IP address> tries to establish HTTP connection.
```

Explanation A security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Action Check for any unauthorized access to the host via the switch through the HTTP connection.

Severity Info

SEC-SECVIOL_TELNET

Message

```
<switch number> Info SEC-SECVIOL_TELNET, 4, Security violation:
  Unauthorized host with IP address <IP address> tries to establish TELNET
  session.
```

Explanation A security violation was reported. The specified unauthorized host attempted to establish a Telnet connection.

Action Check for any unauthorized access to the host via the switch through the Ethernet connection.

Severity Info

39 SECLIB_System Error Messages

This chapter contains the following information:

Introduction

Security Library is a facility used by the FabOS modules. The Security Library provides functionality for enforcement of policies, identification of the switch's role in the fabric, and other tasks. Switch Connection Control (SCC), Device Connection Control (DCC), Management Server (MS), and Internet Protocol (IP) policies are enforced and Fibre Channel Switch (FCS) and non-FCS roles are identified, using the Security Library functions.

SECLIB-SECVIOL_DCC

Message

```
<switch number> Info SECLIB-SECVIOL_DCC, 4, Security violation:
  Unauthorized device <device node name> tries to flogin to port <port
  number> of switch <port node name>.\
```

Explanation A security violation was reported. The specified unauthorized device attempted to f-login to the specified port and switch.

Recommended Action Check DCC policy and verify that the specified device is allowed in the fabric and is included in the DCC policy. If the specified device is not included in the policy, add it to the policy. If the device is not allowed, this is a valid violation message and an unauthorized entity is trying to gain access to your fabric. Action should be taken as mandated by Enterprise Security Policy.

Severity Info

SECLIB-SECVIOL_LOGIN_API

Message

```
<switch number> Info SECLIB-SECVIOL_LOGIN_API, 4, Security violation: Login
   failure attempt via API.  IP Addr: <IP address>
```

Explanation A security violation was reported. The specified unauthorized host attempted to login through an API connection; the login failed.

Action Check API policy and verify that all hosts allowed to access the fabric are included in the API policy. If the host is allowed in the fabric but not included in the policy, add it to the policy.

If the host is not allowed in the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Severity Info

SECLIB-SECVIOL_LOGIN_HTTP

Message

```
<switch number> Info SECLIB-SECVIOL_LOGIN_HTTP, 4, Security violation:
   Login failure attempt via HTTP.  IP Addr: <IP address>
```

Explanation A security violation was reported. The specified unauthorized device attempted to login through an HTTP connection; the login failed.

Action Check the HTTP policy and verify all hosts are allowed access to the fabric are included in the HTTP policy. If the host is allowed in the fabric but not included in the policy, add it to the policy.

If the host is not allowed in the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Severity Info

SECLIB-SECVIOL_LOGIN_MODEM

Message

```
<switch number> Info SECLIB-SECVIOL_LOGIN_MODEM, 4, Security violation:
   Login failure attempt via Modem.
```

Explanation A security violation was reported. An unauthorized device attempted to login through a modem connection; the login failed.

Action Check the Serial Policy and verify the connection is allowed. If the connection is allowed but not specified, allow connection from Serial Policy.

If Serial Policy does not allow connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

The Serial Policy controls both modem and serial access, so enabling access in Serial Policy will enable both modem and serial access.

Severity Info

SECLIB-SECVIOL_LOGIN_REMOTE

Message

```
<switch number> Info SECLIB-SECVIOL_LOGIN_REMOTE, 4, Security violation:
   Login failure attempt via TELNET/SSH/RSH.  IP Addr: <IP address>
```

Explanation A security violation was reported. The specified unauthorized remote device attempted to login through a Telnet or SSH connection; the login failed.

Action Check the Telnet Policy and verify that the hosts allowed access to the fabric through Telnet/SSH are included in the Telnet Policy. If the host is allowed access to the fabric but is not included in the Telnet Policy, add it to the policy.

If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Telnet Policy controls access for both Telnet and SSH connections.

Severity Info

SECLIB-SECVIOL_LOGIN_SERIAL

Message

```
<switch number> Info SECLIB-SECVIOL_LOGIN_SERIAL, 4, Security violation:
   Login failure attempt via SERIAL.
```

Explanation A security violation was reported. An unauthorized device attempted to login through a serial connection; the login failed.

Action Check the Serial Policy and verify the connection is allowed. If the connection is allowed but not specified, allow connection from Serial Policy.

If Serial Policy does not allow connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

The Serial Policy controls both modem and serial access, so enabling access in Serial Policy will enable both modem and serial access.

Severity Info

SECLIB-SECVIOL_MSaccess

Message

```
<switch number> Info ECLIB-SECVIOL_MSaccess, 4, Security violation:
  Unauthorized access from MS device node name <device node name>, device
  port name <device port name>.
```

Explanation A security violation was reported. The specified unauthorized Management Server (MS) device attempted to establish a connection.

Action Check Management Server Policy and verify the connection is allowed. If the connection is allowed but not specified, allow connection in MS Policy.

If MS Policy does not allow connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Severity Info

SECLIB-SECVIOL_MSfwrd

Message

```
<switch number> Info SECLIB-SECVIOL_MSfwrd, 4, Security violation: MS
  command is forwarded from non primary FCS switch.
```

Explanation A security violation was reported. A Management Server command was forwarded from a non-primary FCS switch.

Action No action required.

Severity Info

SECLIB-SECVIOL_MSop

Message

```
<switch number> Info SECLIB-SECVIOL_MSop, 4, Security violation: MS device
  <device wwn> operates on non primary FCS switch.
```

Explanation A security violation was reported. A Management Server device is operating on a non-primary FCS switch.

Action No action required.

Severity Info

SECLIB-SECVIOL_RSNMP

Message

```
<switch number> Info SECLIB-SECVIOL_RSNMP, 4, Security violation:
  Unauthorized host with IP address <IP address> tries to do SNMP read
  operation.
```

Explanation A security violation was reported. The specified unauthorized host attempted to do a Read SNMP operation (RSNMP).

Action Check RSNMP Policy to verify that hosts allowed access to the fabric through SNMP read operations are included in the RSNMP Policy. If the host is allowed access to the fabric but not included in the RSNMP Policy, add the host to the policy.

If host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Severity Info

SECLIB-SECVIOL_SCC

Message

```
<switch number> Info SECLIB-SECVIOL_SCC, 4, Security violation:
  Unauthorized switch <switch wwn> tries to join secure fabric.
```

Explanation A security violation was reported. The specified unauthorized switch attempts to join the secure fabric.

Action Check the Security Connection Control Policy (SCC Policy specifies the WWNs of switches allowed in the fabric) to verify which switches are allowed in the fabric. If the switch is allowed in the fabric but not included in the SCC Policy, add the switch to the policy.

If the switch is not allowed in the fabric, this is a valid violation message and an unauthorized entity is trying to access the fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Severity Info

SECLIB-SECVIOL_WSNMP

Message

```
<switch number> Info SECLIB-SECVIOL_WSNMP, 4, Security violation:
  Unauthorized host with IP address <IP address> tries to do SNMP write
  operation.
```

Explanation A security violation was reported. The specified unauthorized host attempted to do a write SNMP operation (WSNMP).

Action Check the WSNMP Policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy.

If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Appropriate action should be taken as mandated by your Enterprise Security Policy.

Severity Info

40 SEMA_System Error Messages

This chapter contains the following information:

Introduction

Semaphore (SEMA) is used to control the flow of data traffic, so that traffic flow does not overlap and crash the software.

SEMA-SEMGIVE

Message

```
<switch number> Critical SEMA-SEMGIVE, 1, semaGive, sema = <semaphore>,
   errno = <error number>
```

Explanation A failure occurred when releasing a semaphore from the queue. The *<semaphore>* provides which semaphore had the error, and *<error number>* is the internal error number used for debugging.

Action Copy the error message and contact EMC Customer Support Center.

Severity Critical

SEMA-SEMTAKE

Message

```
<switch number> Critical SEMA-SEMTAKE, 1, semaTake, sema = <semaphore>,
   errno = <error number>
```

Explanation A failure occurred when taking a semaphore. The *<semaphore>* provides which semaphore had the error, and *<error number>* is the internal error number used for debugging.

Action Copy the error message and contact EMC Customer Support Center.

Severity Critical

41 SULIB_System Error Messages

This chapter contains the following information:

Introduction

Software Upgrade Library provides the `firmwaredownload` command capability, which downloads firmware to both CP cards with a single command. The following error messages might be seen if there are any problems during the firmwaredownload procedure, when the firmware is being downloaded to both CPs. General outline of the firmware download procedure: first the new fiw is downloaded to the standby CP. Once the new fw is deemed "good", the active CP automatically fails over and the standby CP takes over. The new fw is then downloaded to the now standby CP, and when the fw is "good", CP2 fails over and CP1 is again the active CP. For additional information, refer to the *Fabric OS Procedures Manual*, Firmware Download chapter.

SULIB-ACTIVE_FAILOVER

Message

```
<switch number> Info SULIB-ACTIVE_FAILOVER, 4, Active CP forced failover
   succeeded. This CP is now active.
```

Explanation The forced failover was successful, and the standby CP is now the active CP. An informational message.

Recommended Action No action required. The `firmwaredownload` command is progressing as expected.

Severity Info

SULIB-CP_REBOOT

Message

```
<switch number> Info SULIB-CP_REBOOT, 4, Standby CP reboots.
```

Explanation The standby CP will reboot. An informational message.

Action No action required. The `firmwaredownload` command is progressing as expected.

Severity Info

SULIB-CP_REBOOT_OK

Message

```
<switch number> Info SULIB-CP_REBOOT_OK, 4, Standby CP rebooted
  successfully.
```

Explanation The standby CP has rebooted successfully. An informational message.

Action No action required. The `firmwaredownload` command is progressing as expected.

Severity Info

SULIB-FWDL_END

Message

```
<switch number> Warning SULIB-FWDL_END, 3, FirmwareDownload has completed
   successfully
```

Explanation The firmware download was completed successfully to the both CPs. An informational message.

Action No action required. The `firmwaredownload` command has completed as expected.

Severity Warning

SULIB-FWDL_FAIL

Message

```
<switch number> Info SULIB-FWDL_FAIL, 4, FirmwareDownload failed
   (status=<error message>).
```

Explanation The firmware download failed. The additional *<error message>* information provides debugging information.

Action Call EMC Customer Support or see the *Fabric OS Procedures Guide* for troubleshooting information.

Severity Info

SULIB-FWDL_START

Message

```
<switch number> Warning SULIB-FWDL_START, 3, FirmwareDownload has started.
```

Explanation The firmware download has started.

Action Do not failover or power down the system during firmware download. Allow the command to continue without disruption. No action required.

Severity Warning

42 SWITCH_System Error Messages

This chapter contains the following information:

Introduction

SWITCH messages are generated by the switch driver module that manages a Fibre Channel Switch instance.

SWITCH-SECVIOL_DCC

Message

```
<switch number> Info SWITCH-SECVIOL_DCC, 4, Security violation:
  Unauthorized device <WWN> tries to flogin to port <port number>
```

Explanation A security violation was reported. The specified unauthorized device (specified by the <*WWN*>) attempted to flogin to the specified secure port.

Recommended Action Check the Security Policy to verify \ the device is allowed in the fabric. If device is allowed, add device to Security Policy and connect to the appropriate port. If device is not allowed, this is a valid security violation notification and appropriate action should be taken as mandated in the Enterprise Security Policy.

Severity Info

43 SYSC_System Error Messages

This chapter contains the following information:

Introduction

System Controller is a daemon that starts up and shuts down all FabOS modules in the proper sequence.

SYSC-ERROR

Message

<switch number> `Critical SYSC-ERROR, 1,` *<error information>*

Explanation The *<error information>* indicates where the source of the error is and is used for troubleshooting.

Recommended Action Copy the error message, run `hadump` and `errdump` and contact EMC Customer Support Center.

On bladed switches, run `hadump` on both CP Cards.

Severity Critical

SYSC-LAUNCHFAIL

Message

```
<switch number> Critical SYSC-ERROR, 1, Could not launch <error information>
```

Explanation This message is logged during the boot sequence when one of the programs would not run on the system. The *<error information>* indicates where the source of the error is and is used for troubleshooting.

Recommended Action If the message is reported during a reboot after a new firmware has been loaded, try reloading the firmware.

If the problem still persists, there may be a conflict between the two versions of firmware or the flash may be corrupted. contact EMC Customer Support Center with:

- the exact error message,
- the firmware version that was loaded on the switch before the error occurred, and
- the firmware version you are trying to load.

Severity Critical

44 TRACK_System Error Messages

This chapter contains the following information:

Introduction

The Track Change feature tracks the following events:

- Turning on or off the Track Change feature.
- CONFIG_CHANGE
- LOGIN
- LOGOUT
- FAILED_LOGIN

If any of the above events occur, then a message is sent to the error log. Additionally, if the SNMP Trap option is enabled, an SNMP Trap is also sent (for more information on the Track Change feature and SNMP traps, see the Fabric OS Reference).

For information on configuring the Track Change feature, refer to the *Fabric OS Reference Guide*, or the *Fabric OS Procedures Guide*.

TRACK-CONFIG_CHANGE

Message

```
<switch number> Info TRACK-CONFIG_CHANGE, 4, Config file change from task:
  <task>
```

Explanation The switch configuration has changed from the specified task. The following variables will be displayed in the error message:

- *<switch number>*
  For the ED-12000B: may be 0 or 1.
  For the DS-32B2: will be 0.
- *<task>*
  PDMIPC:

Recommended Action None. Information only; the message can be ignored. To see the new configuration, use `configshow`.

Severity Info

TRACK-FAILED_LOGIN

Message

```
<switch number> Info TRACK-FAILED_LOGIN, 4, Unsuccessful login
```

Explanation Login attempt to the specified switch is unsuccessful. This may happen if the user name or password is wrong.

In the message above, the *<switch number>* variable for an ED-12000B may be 0 or 1; for aDS-32B2 it is 0.

Recommended Action Verify that the user name and password are correct.

Severity Info

TRACK-LOGIN

Message

```
<switch number> Info TRACK-LOGIN, 4, Successful login
```

Explanation The specified switch reported a successful login.

In the message above, the *<switch number>* variable for an ED-12000B 12000 may be 0 or 1; for a DS-32B2 it is 0.

Recommended Action None

Severity Info

TRACK-LOGOUT

Message

```
<switch number> Info TRACK-LOGOUT, 4, Successful logout
```

Explanation The specified switch reported a successful logout.

In the message above, the *<switch number>* variable for an ED-12000B may be 0 or 1; for a DS-32B2 it is 0.

Recommended Action None

Severity Info

TRACK-TRACK_OFF

Message

```
<switch number> Info TRACK-TRACK_OFF, 4, Track-changes off
```

Explanation The Track Change feature has been turned off.

In the message above, the *<switch number>* variable for an ED-12000B may be 0 or 1; for a DS-32B2 it is 0.

Recommended Action None. Refer to *Fabric OS Procedures Guide* to turn the Track Change feature back on.

Severity Info

TRACK-TRACK_ON

Message

```
<switch number> Info TRACK-TRACK_ON, 4, Track-changes on
```

Explanation The Track Change feature has been turned on.

In the message above, the <*switch number*> variable for an ED-12000B may be 0 or 1; for a DS-32B2 it is 0.

Recommended Action None. Refer to *Fabric OS Procedures Guide* to turn the Track Change feature off.

Severity Info

45

TS_System Error Messages

This chapter contains the following information:

Introduction

Time Service provides fabric time synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.

TS-CLKSVRERR

Message

```
<switch number> Warning TS-CLKSVRERR, 3, <%s> Clock Server used instead of
  <number>: locl: <domain> remote: <domain>
```

Explanation The fabric time synchronization was not distributed from the principal switch. Instead, an alternate server was used.

Recommended Action None

Severity Warning

TS-NTPQFAIL

Message

```
<switch number> Warning TS-NTPQFAIL, 3, NTP Query failed: <err code>
```

Explanation The NTP query to external server failed. Clock server will be set to LOCL.

Recommended Action Verify that clock server address is valid and clock server is available. If specified clock server is not available, point to an available server.

Severity Warning

TS-SEND_FAIL

Message

```
<switch number> Warning TS-SEND_FAIL, 3, <domain> Send failed with error
  code <error number>.
```

Explanation The Time Server send failed.

Recommended Action See Fabric Watch for more information.

Severity Warning

TS-TSINFO

Message

```
<switch number> Info TS-TSINFO, 4, Init failed. Time Service exiting.
```

Explanation Time server was started in error. Attempt failed.

Recommended Action None

Severity Info

TS-TS_SVR_ERRCODE_EXITS

Message

```
<switch number> Warning TS-CLKSVRERR, 3, <domain> Clock Server used instead
  of <switch>: locl: <domain> remote: <domain>
```

Explanation The Time Server error code is exiting.

Recommended Action See Fabric Watch for more information.

Severity Warning

TS-TSSVREXITS

Message

```
<switch number> Warning TS-TSSVREXITS, 3, <domain>: TS Server Exiting...
```

Explanation The Time Server is exiting.

Recommended Action See Fabric Watch for more information.

Severity Warning

TS-WARN

Message

```
<switch number> Warning TS-WARN, 3, <reason>
```

Explanation The Time Server is reporting a warning for the specified reason.

Recommended Action See Fabric Watch for more information.

Severity Warning

46

UCAST_System Error Messages

This chapter contains the following information:

Introduction

UCAST is a part of the FSPF (Fabric Shortest Path First) protocol that manages the Unicast routing table.

UCAST-DOUBLEPATH

Message

```
<switch number> Debug UCAST-DOUBLEPATH, 5, Duplicate Path to Domain <domain
   ID>, Output Port = <port number>, PDB pointer = <value>
```

Explanation Duplicate paths were reported to the specified domain from the specified output port. The path database (PDB) pointer is the address of the path database and provides debugging information.

Action No user action required.

Severity Debug

47 UPATH_System Error Messages

This chapter contains the following information:

Introduction

UPATH is a part of the FSPF (Fabric Shortest Path First) protocol that uses the SPF algorithm to dynamically compute a unicast tree.

UPATH-UNREACHABLE

Message

```
<switch number> Warning UPATH-UNREACHABLE, 3, No minimum cost path in
   candidate list
```

Explanation The specified switch *<switch number>* is unreachable because no minimum cost path (FSPF UPATH) exists in the candidate list (domain ID list).

Action This will end the current SPF computation and no user action is required.

Severity Warning

48

uSWD_System Error Messages

This chapter contains the following information:

Introduction

The Userspace Software Watch Dog daemon informs kSWD about which daemons the watchdog subsystem will monitor. Additionally, the uSWD daemon helps the kSWD daemon to print debug information if a Critical daemon has an unexpected termination.

uSWD-APP_NOT_REFRESH_ERR

Message

```
<switch number> Critical uSWD-APP_NOT_REFRESH_ERR, 1, (uSWD)Application
  with pid <number> not refreshing watchdog.
```

Explanation A critical error occurred in the Watch Dog subsystem. An application is not able to refresh. Refer to the specified PID number to find out which application is failing. The switch will reboot (on single-CP switches) or fail-over (on dual-CP switches).

Action Run the `savecore` command to find if a Core File was created. If a Core File is found, select the *FTP the file* option.

Copy the error message and contact customer support.

Severity Critical

uSWD-uSWD_GENERIC_ERR_CRITICAL (uSWD)

Message

```
<switch number> Critical uSWD-uSWD_GENERIC_ERR_CRITICAL, 1, uSWD: <error
  message>
```

Explanation A critical application error was reported in the Watch Dog subsystem. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or fail-over (on dual-CP switches).

The <error message> may be any one of the following messages:

- <swd_read_conf() Failed!>
  Explanation: Unable to read the list of applications (daemons) that needs to be monitored.
- <Opening sys module has Failed <number>>
  Explanation: Internal error on device number.
- <Can't get number of switches!>
  Explanation: Internal error condition.
- <Can't open SWD device>
  Explanation: Internal error condition. Unable to open the watchdog device.
- <Registering SCN has Failed, status = <number> error = <number>>
  Explanation: Internal error condition.
- <SWD_USER: sysModGetFd Failed<number>>
  Explanation: Internal error condition.

Action Run the `savecore` command to find if a Core File was created. If a Core File is found, select the *FTP the file* option.

Copy the error message and contact customer support.

Severity Critical

A

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure A-1).

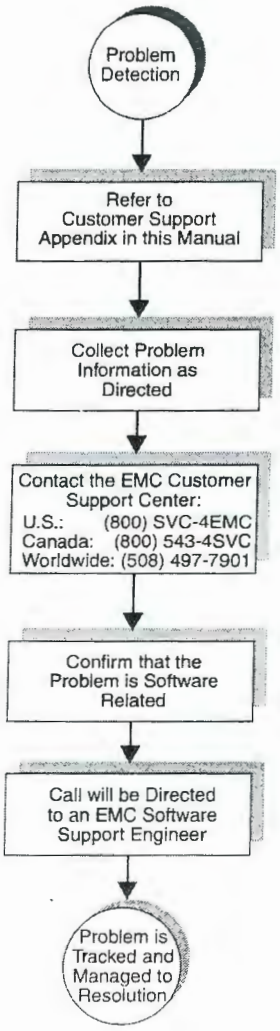


Figure A-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

```
http://powerlink.emc.com
```

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. 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 See *Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode*.

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit*.

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL*.

M

Media See *Transceiver*.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port*.

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A Brocade product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

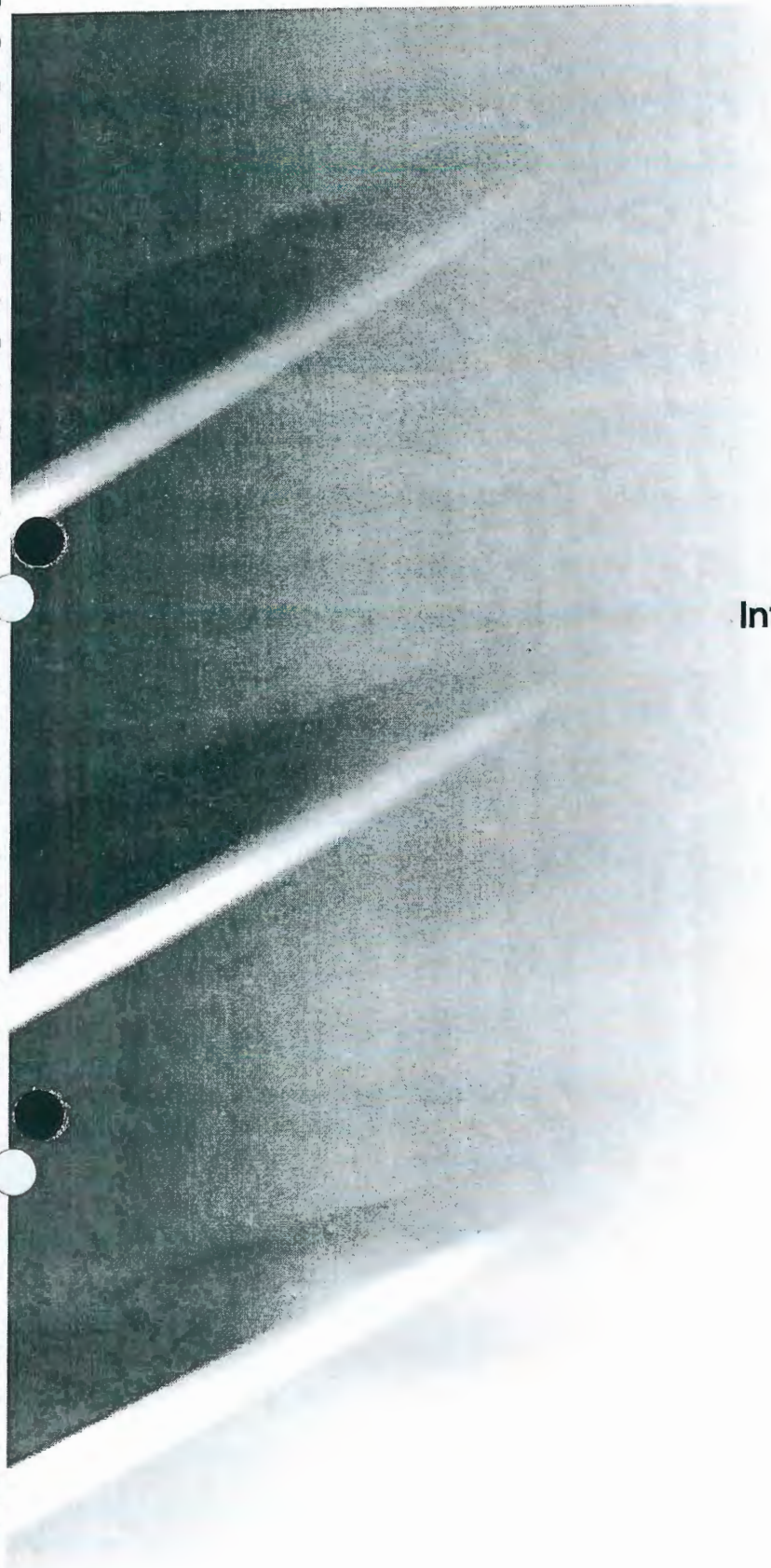
Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ANEXO SWITCH TIPO 03
PARTE 11

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br



EMC Connectrix B Series
Interswitch Link (ISL) Trunking
Version 3.1 and Version 4.1

USER GUIDE

P/N 300-000-642
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

EMC Connectrix B Series systems have been extensively tested and certified to meet UL1950, CSA 22.2 No 950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Preface

Interswitch Link (ISL) Trunking is an optionally licensed product that requires a valid license key to function. It is supported for the EMC Connectrix Series B switches, using any EMC qualified version of Fabric OS.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix B Series Fabric OS. Therefore, some functions described in this guide may not be supported by all versions currently in use. For the most up-to-date information on product features, see the product release notes.

If a DS-16B2, DS-32B2, and ED-12000B switch feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance.

Audience

This guide is part of the EMC Connectrix B Series documentation set, and is intended for use by the switch administrator during installation and configuration of the switch.

Readers of this guide are expected to be familiar with the EMC Connectrix B series operating environment.

Organization

Here is an overview of where information is located in this guide.

- Chapter 1, *Introducing ISL Trunking*, provides an overview of the ISL Trunking feature.
- Chapter 2, *Installing ISL Trunking*, provides instructions for installing an ISL Trunking license key.

- Chapter 3, *Using ISL Trunking*, provides information on how to use the ISL Trunking feature with Telnet commands or Web Tools. This chapter also includes a section that covers frequently asked questions.
- Appendix B, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix B series.
- The *Glossary* defines terminology used in this manual.

Related Documentation

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-16B2 QuickLoop Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*

- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this guide:

Palatino, bold	• Dialog box, button, icon, and menu items in procedures • Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	• New terms or unique word usage in text • Command line arguments when used in text • Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	User entry. For example: **`symmpoll -p`**
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC website at:

`http://www.emc.com/contact/`

For additional information, refer to the EMC Powerlink website at:

`http://powerlink.emc.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to **`techpub_comments@emc.com`** with your opinions of this guide.

1 Introducing ISL Trunking

This chapter provides the following information:

Overview

Interswitch Link (ISL) Trunking is an optionally licensed product available on the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B with any EMC qualified version of Fabric OS. You can manage ISL Trunking using Telnet commands or the Web Tools interface.

The ISL Trunking feature allows up to four ISL connections between two switches through an expansion port (E_Port), to merge logically into a single link. With ISL Trunking, high-speed links ensure that server-to-storage performance is efficient and shared under heavy network loads. When using ISL Trunking to aggregate bandwidth of up to four ports, the speed of the ISLs between switches in a fabric is quadrupled. ISL Trunking delivers ISL throughput of up to 8 Gb/s if four ISLs are used.

The primary task of ISL Trunking is to route data between edge switches that aggregate connections to servers and storage. ISL Trunking also supports high-bandwith, large scale SANs, which include core switches that interconnect with other switches.

For a list of frequently asked questions about the ISL Trunking Feature, refer to *Frequently Asked Questions About ISL Trunking* on page 3-16.

Advantages of ISL Trunking

The ISL Trunking feature enhances switch-to-switch performance in Storage Area Networks while simplifying management and improving reliability. Advantages of the ISL Trunking feature include:

- Combining up to four ISLs into a single logical ISL
- Load sharing traffic across all ISLs in a trunk
- Maintaining in-order delivery of frames
- Avoiding rerouting if one of the server links between two switches fails; however, rerouting occurs when a trunk master is down
- Simplifying management by implementing fewer ISLs

Routing Without the ISL Trunking Feature

Prior to the implementation of the ISL Trunking feature, device-level load sharing was done through Fibre Channel networks that created ISLs and operated with the Fibre Channel Shortest Path First (FSPF) routing protocol. The protocol established and communicated the shortest paths for data to be carried from source to destination. Load sharing multiple ISLs to connect two switches was established by a round robin algorithm that assigned the next available ISL as part of the link to connect a host bus adapter (HBA) and storage.

Depending on the fabric event sequences, multiple HBAs shared an individual ISL. This type of load sharing sometimes caused the fabric to have congested input/output traffic over the ISLs connecting two switches.

Although FSPF-compliant switches ensure fixed routing paths, and guarantee that all frames are delivered in order, congestion occurs if the aggregation of the stream exceeds the capacity of one of the ISLs in the path.

For example, Figure 1-1 shows four untrunked ISLs with a maximum capacity of 2 Gb/s each, for a maximum throughput of 8 Gb/s. Due to traffic that is not trunked, the throughput of the four ISLs is:

1 Gb/s + 1.5 Gb/s + 0.5 G + 1 Gb/s + 1 Gb/s

giving a total of only 5 Gb/s, because two 2 Gb/s data streams are competing for the same path.

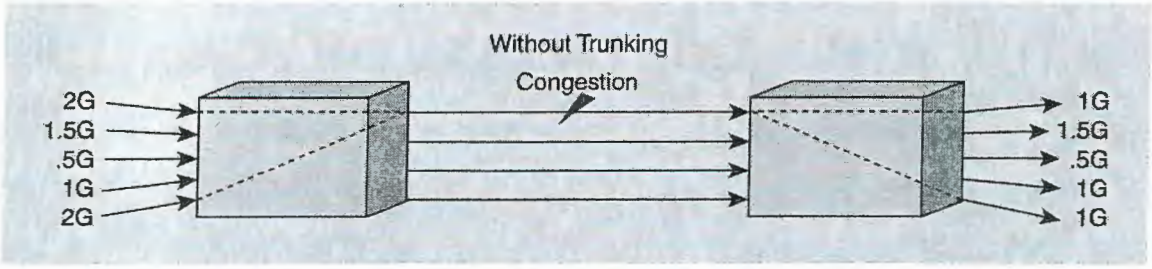


Figure 1-1 Routing Without the ISL Trunking Feature

Routing With the ISL Trunking Feature

ISL Trunking ensures that all links are used efficiently, eliminating congestion on one link, while distributing the load of the links. This feature is designed to significantly reduce traffic congestion. As shown in Figure 1-2, four ISLs are combined into a single logical ISL with a total capacity of 8 Gb/s.

The ISL Trunking feature improves the Fabric Shortest Path First (FSPF) concept by preventing the loss of a link in a route. With trunking, a link failure merely reduces the available bandwidth of the logical ISL trunk. In other words, a failure does not completely "break the pipe," but simply makes the pipe thinner. As a result, data traffic is much less likely to be affected by link failures and the bandwidth automatically increases when repaired.

ISL Trunking uses *deskew values*, which are a measure of the latency differences between ISL cables in the same group, to provide in-order delivery of traffic. Deskew values are automatically calculated at the creation of each new trunking group.

The ISL Trunking feature distributes the workload across all ISLs in a trunk. Each incoming frame is sent across the first available ISL. As a

result, transient workload peaks for one system or application are much less likely to impact the performance of other parts of the SAN fabric. Because the full bandwidth of each physical link is available, bandwidth is efficiently allocated.

In Figure 1-2, four ISLs provide 8 Gb/s of total throughput. With the implementation of ISL Trunking, bandwidth is shared across the trunked ISLs, permitting a total throughput of 2 Gb/s + 1.5 Gb/s + 0.5 Gb/s + 1 Gb/s + 2 Gb/s, or 7 Gb/s. Because the trunk aggregates the four individual paths into one and preserves it in the order delivery of frames, the total throughput is increased compared to a nontrunked group of ISLs.

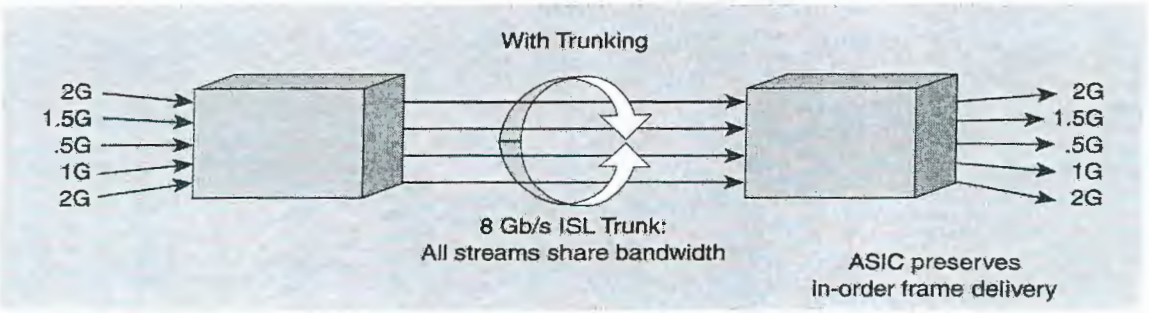


Figure 1-2 Routing With the ISL Trunking Feature

Trunking Groups, Ports, and Masters

ISL Trunking dynamically performs load sharing, at the frame level, across a set of available links between two adjacent switches to establish a trunking group. Ports that belong to a trunking group are called *trunking ports*. One port is used to assign traffic for the group, and is referred to as the *trunking master*.

ISL trunking can only be established with any combination of these switches: DS-16B2, DS-32B2, and ED-12000B. It cannot be established with older DS-16B or DS-8B switches.

Trunking Groups

A trunking group is a set of links that distribute frames across a set of available paths linking two adjacent switches. When two, three, or four adjacent ISLs are used to connect two switches, the switches automatically group the ISLs into a single logical ISL. A trunking group is identified by the trunking master that represents the entire group. Non-master trunking ports from a trunking group are referred to as slave links that help the trunking master direct traffic across ISLs, allowing efficient and shared in-order communication. Failure of a slave port has minimal impact on the traffic flow of the trunk.

Trunking Ports

Trunking ports are grouped by four adjacent ports that share a common pool of frame buffers on a quad. When connecting two switches in a fabric with ISLs, consider leaving other ports open on the quad for future trunk growth and/or sparing.

Trunking ports in a trunking group must meet the following criteria:

- Ports must be capable of becoming E_Ports, which are used to connect to other switches. E_Ports communicate in Class F frames to distribute information about the different servers and to set up circuits that pass frames to the appropriate nodes over the fabric.
- Ports must reside in the same contiguous four-port groups. For example: 0-3, 4-7, 8-11, 12-15. All ports in the same trunking group must reside in the same quad; quads are groups of four adjacent ports that are marked in intervals on each switch. The first four ports on a switch comprise the first quad, and every group of four adjacent ports thereafter comprise another quad. Figure 1-3 though Figure 1-5 show the quads for various switch models.

- Ports must be set to run at the 2 G speed. The port speed can be set to auto-negotiation speed.
- The cable difference between all ports in a trunking group must be less than 400 meters, and should be kept to 30 meters or less within a trunk to ensure optimal performance and bandwidth use.
- If Extended Fabrics is in use, the ports must be in the L0 mode. ISL Trunking does not support the LE, L1, or L2 portcfglongdistance modes. For information about these modes and Extended Fabrics, refer to *Extended Fabrics User Guide*.

Potential trunking groups are marked on the front of the switch, according to quad location. Figure 1-3 shows which ports on a DS-16B2 belong to the same quads.

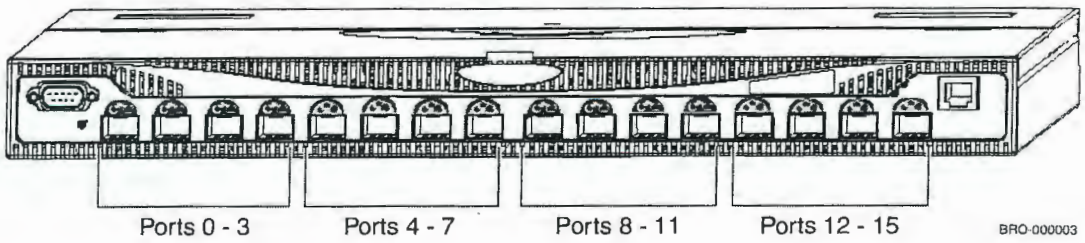


Figure 1-3 Quad and Port Groupings on a DS-16B2

Figure 1-4 shows which ports on a DS-32B2 belong to the same quads.

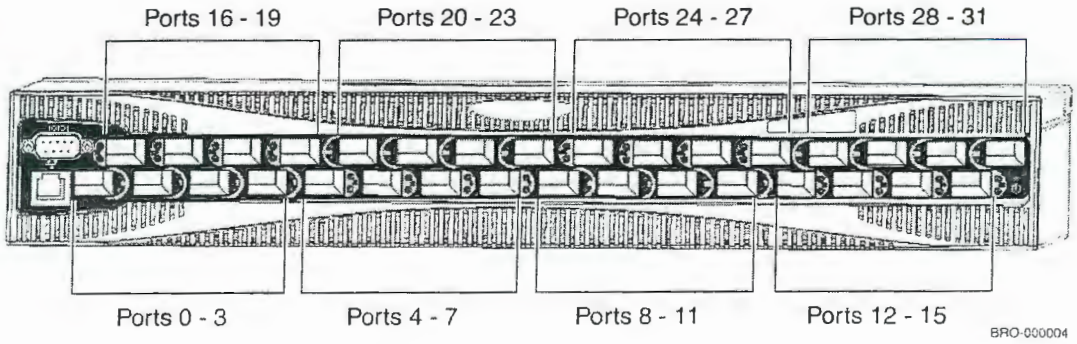


Figure 1-4 Quad and Port Groupings on a DS-32B2

Figure 1-5 shows which ports on an ED-12000B port card belong to the same quads.

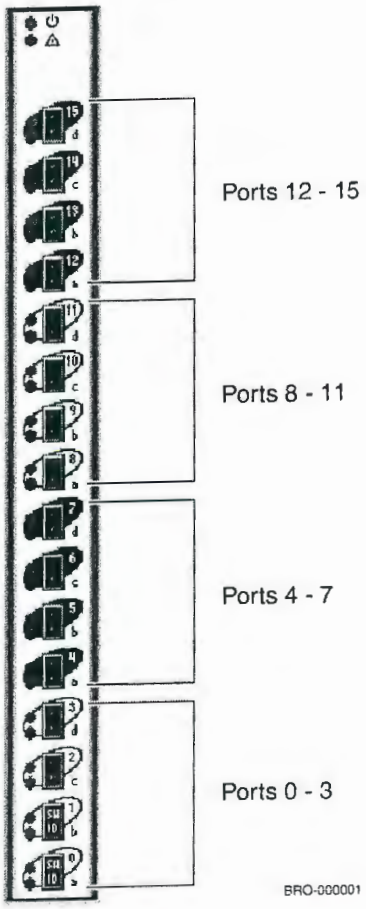


Figure 1-5 Port Groupings on the Port Card of an ED-12000B

Trunking Masters

Only one of the trunking ports is used to set up all routing paths for an entire trunking group, this port is called the trunking master port. The trunking master implicitly defines the trunking group. Each trunking group includes a single trunking master and from one to three trunking slave links.

The first ISL found in any trunking group is assigned to be the trunking master. There can be several trunks, each with one master port, between two adjacent switches; however, there is only one

designated principal (master) ISL between the switches. After the trunking group is fully established, all data packets intended for transmission across the trunk are dynamically distributed at the frame level across the ISLs in the trunking group, while preserving in-order delivery.

When a master trunking link goes off line or fails, and there are at least two remaining active trunking ports, the remaining slave links go off line and regroup with a new master.

2 Installing ISL Trunking

This chapter provides the following information:

Overview

Installing the ISL Trunking feature involves the purchase and activation of a license for each switch you want to enable for trunking. After the license is activated and the port is enabled for trunking, ISL Trunking is automatically invoked as ISLs are added between two 2 Gb/s switches. To see whether an ISL Trunking license is installed, perform the steps in the next section, *Installing ISL Trunking Through Telnet*. If an ISL Trunking license has not been installed, contact your EMC Sales Representative to obtain a license key.

With this feature, you must obtain a license key for each switch using the EMC ISL Trunking feature.

The ISL Trunking feature can only be established with any combination of these switches: DS-16B2, DS-32B2, and ED-12000B running any qualified version of Fabric OS. A Trunking license can be installed using either Telnet, Web Tools, or Fabric Manager.

Trunking is only supported for normal E_Ports (referred to as L0 in the portcfglongdistance command) up to 5 km at the full speed permitted by the link. For information about these modes and Extended Fabrics in general, refer to the *Extended Fabrics User Guide*.

Installing ISL Trunking Through Telnet

To use Telnet to log on to the ISL Trunking feature:

From a command prompt screen, use the Telnet command to log on to the switch (refer to the *appropriate Fabric OS Reference Guide* provided with the hardware for details), using an account that has administrative privileges.

1. Determine whether an ISL Trunking license is already installed on the switch by typing **`licenseShow`** on the Telnet command line.

   The command displays all of the licenses currently installed on the switch. For example:

   ```
   admin> licenseShow
   1A1AaAaaaAAAA1a:
   Fabric License
   Web license
   Zoning license
   Trunking license
   ```

   If the Trunking license is not included in the list, continue with step 2.

2. Enter the following on the command line:

   `licenseAdd "key"`

   where *"key"* is the license key provided to you. The license key is case sensitive and must be entered exactly as given.

3. Verify the license was added by entering the following on the command line:

   `licenseShow`

   If the ISL Trunking license is listed, the feature is installed and immediately available.

   If the license is not listed, repeat step 2 after verifying that the license being added is for the correct switch. Licenses are only valid for one particular switch.

Installing ISL Trunking Through Web Tools

To enter the ISL Trunking license key using the Web Tool user interface:

1. Launch the web browser, by entering the switch name or IP address in the **Location/Address** field, and pressing ENTER.

   Web Tools launches, displaying the Fabric View.

2. Click **Admin View** on the relevant switch panel.

   The logon window displays.

3. Enter a logon name and password with administrative privileges and press ENTER.

   The Switch Admin view displays.

4. Click the **License Admin** tab, enter the license key in the **License Key** field, and click **Add**.

   The ISL Trunking feature is available as soon as the license key is added.

Implementing Trunking in the Fabric

To use ISL Trunking in the fabric, the fabric must be designed to allow trunking groups to form. To identify the most useful trunking groups, evaluate the traffic patterns before designing/redesigning the fabric.

ISL Trunking is enabled by default for each port on the switch as shipped. For instructions on disabling and enabling trunking capability for individual ports or all the ports on the switch, see *Enabling and Disabling Trunking* on page 3-4.

Designing the Fabric to Optimize Use of ISL Trunking

ISL Trunking can be used to simplify SAN (storage area network) design and improve performance. When designing the SAN, consider the following recommendations in addition to the standard guidelines for SAN design:

- Evaluate the traffic patterns within the fabric. This allows implementation of trunking groups that will help to optimize fabric performance. Refer to *Evaluating Data Traffic Patterns* on page 2-6 for more information.

- Place trunking-capable switches adjacent to each other. This maximizes the number of trunking groups that can form. If using a core/edge topology, place trunking-capable switches at the core of the fabric and any switches that are not trunking-capable at the edge of the fabric.
- Activate an ISL Trunking license on each switch that is expected to participate in a trunking group.
- The lengths of the ISLs in the group should differ by less than 30 meters (recommended), and must differ by less than 400 meters. This is because large differences in latency decrease the efficiency of load-sharing. If cable lengths differ by 400 meters or more, the trunking group forms only for the ISLs that have lengths that differ by less than 400 meters.
- When connecting two switches with two or more ISLs, ensure that all trunking requirements are met to allow a trunking group to form.
- Determine the optimal number of trunking groups between each set of linked switches, depending on traffic patterns and port availability. The goal is to avoid traffic congestion without unnecessarily using ports that could be used to attach other switches or devices.

  Considerations:

  - Each physical ISL uses 2 ports that could otherwise be used to attach node devices or other switches.
  - Trunking groups can be used to resolve ISL oversubscription if the total capability of the trunking group is not exceeded.
- Consider how the addition of a new path will affect existing traffic patterns:
  - A trunking group has the same link cost as the master ISL of the group, regardless of the number of ISLs in the group. This allows subordinate ISLs to be added or removed without causing data to be re-routed, since the link cost remains constant.
  - The addition of a path that has less link cost than existing paths causes traffic to be re-routed through that path.
  - The addition of a path that has more link cost than existing paths may not be useful since the traffic will choose the shorter paths first.

- For trunking groups over which traffic is likely to increase as business requirements grow, consider leaving one or two ports in the quad available, for future use as a non-disruptive addition of bandwidth to that trunk.
- Consider creating redundant trunking groups where additional ports are available or paths are particularly critical. This helps to protect against oversubscription of trunking groups, multiple ISL failures in the same group, and the rare occurrence of an ASIC failure.
- To provide the highest level of reliability, deploy trunking groups in redundant fabrics to further ensure ISL failures do not disrupt business operations.

SWL and LWL fiber optic cables and transceivers can be used in the same trunking group.

Evaluating Data Traffic Patterns

Traffic patterns can be monitored using the `portperfshow` command, the Performance Monitoring feature, the Fabric Watch feature, or a combination.

Using the CLI to Gather Traffic Data

The `portperfshow` command can be used to record the traffic volume for each port over time to identify the congested paths that would benefit from the implementation of trunking groups. This command can also be used to identify frequently dropped links, so that troubleshooting can be performed and the links can be added back to trunking groups as necessary.

To use the portperfshow command to gather traffic data:

1. Open a serial or telnet connection to one of the central switches in the fabric.
2. Log into the switch as admin.
3. Enter the following:

   `portperfshow` *[interval]*

   interval is the number of seconds between each sample. If no interval is specified, the frequency defaults to one sample every 1 second.
4. Record the traffic flow for each port that is participating in an ISL.

5. Repeat step 1 through step 4 for the other switches in the fabric as required, until all ISL traffic flow is captured (in a very large fabric, it may be necessary to identify and capture the key ISLs, only to save time).
6. Repeat step 1 through step 5 throughout the day (or entire work cycle) to capture varying traffic patterns.

The following example shows traffic flowing through a trunking group of three ports, with one of the links failing after the second reading, causing redistribution of traffic over the remaining two links in the group.

```
switch:admin> portperfshow

0    1    2    3    4    5    6    7    8    9   10   11   12   13   14  15  Total
-------------------------------------------------------------------------------------
   -----
  0    0    0  145  140  245  220  240  145  140  145  120  120  145  145 140  2090
  0    0    0  140  145  220    0  220  115  120  240  145  145  140    0   0  1630
  0    0    0    0  145  240  245  220    0  145    0    0  145    0  140   0  1280
  0    0    0  145  140  245  220  210  125  120  145  120  120  145  145 140  2020
  0    0    0  140  145  220    0  220  115  120  240  145  145  140    0   0  1630
  0    0    0  145  140  245  220  240  145  140  145  120  120  145  145 140  2090
  0    0    0    0  145  240  245  220    0  145    0    0  145    0  140   0  1280
  0    0    0  145  140  245  220  240  145  140  145  120  120  145  145 140  2090

switch:admin>

switch:admin> portperfshow

0    1    2    3    4    5    6    7    8    9   10   11   12   13   14  15  Total
-------------------------------------------------------------------------------------
   -----
  0    0    0    0    0  145  144  145    0    0    0    0    0    0    0   0   434
  0    0    0    0    0  144  143  144    0    0    0    0    0    0    0   0   431
  0    0    0    0    0  162    0  162    0    0    0    0    0    0    0   0   324
  0    0    0    0    0  186    0  186    0    0    0    0    0    0    0   0   372
  0    0    0    0    0  193    0  192    0    0    0    0    0    0    0   0   385
  0    0    0    0    0  202    0  202    0    0    0    0    0    0    0   0   404
  0    0    0    0    0  209    0  209    0    0    0    0    0    0    0   0   418

switch:admin>
```

For more details about this command, refer to the appropriate *Fabric OS Reference Manual*.

Using Performance Monitoring to Gather Traffic Data

Performance Monitoring can be used to monitor traffic flow and to view the impact of different fabric configurations on performance.

For instructions on using Performance Monitoring, refer to the *Performance Monitoring User Guide*.

Using Fabric Watch to Gather Traffic Data

Fabric Watch can be used to monitor traffic flow through specified ports on the switch and send alerts when the traffic exceeds or drops below configurable thresholds. This allows the administrator to monitor changes in traffic patterns and adjust the fabric design accordingly, such as by adding, removing, or reconfiguring ISLs and trunking groups.

For instructions on configuring Fabric Watch thresholds and alerts, refer to the *Fabric Watch User Guide*.

3 Using ISL Trunking

This chapter provides the following information:

Overview

Users manage the ISL Trunking feature by performing some administration tasks. These tasks include:

- Enabling or disabling the trunking
- Enabling and disabling ports of a switch
- Setting the speed of a port
- Debugging a trunking link failure

Administering ISL Trunking

ISL Trunking optimizes the use of ISLs and reduces the SAN administration effort. Given two SANs of equivalent functionality, the SAN that is easier to manage has the advantage. Because ISLs are managed as a group, instead of individually, the EMC ISL Trunking feature minimizes the effort of managing an SAN.

The EMC ISL Trunking feature can be administered using Telnet commands or through EMC Web Tools.

Enabling and Disabling Trunking

Trunking can be enabled and disabled for an individual port or an entire switch, through either the CLI or Web Tools.

Enabling and Disabling Trunking Through the Command Line Interface

Telnet and serial sessions can be used to enable and disable trunking.

To enable or disable trunking for an individual port:

1. Open a CLI connection to the switch to be modified.
2. Log into the switch as admin.
3. Enter the following:

   portcfgtrunkport *slotnumber/portnumber 1 | 0*

   slotnumber = Specify number of slot in which the port card containing the port is located; only required for ED- 12000B

   portnumber = Specify port number on which to enable or disable trunking

   1 | 0 = Enable/disable trunking; specify 1 to enable this port for trunking, or 0 to disable this port for trunking

Example Enabling trunking for port 3 in slot 1:

```
switch:admin> portcfgtrunkport 1/3 1
 done.
switch:admin>
```

To enable or disable trunking for ALL the ports on a switch:

1. Open a CLI connection to the switch to be modified.
2. Log into the switch as admin.
3. Enter the following:

   switchcfgtrunk *1 | 0*

   1 | 0 = Enables or disables trunking; specify "1" to enable trunking on all ports in the switch, or "0" to disable trunking on all ports in the switch

To enable all ports on the switch for trunking:

```
switch:admin> switchcfgtrunk 1
Committing configuration...done.
switch:admin>
```

ISL Trunking Telnet Commands

Table 3-1 lists the Telnet commands used to manage the EMC ISL Trunking Feature when running Fabric OS v4.1. For detailed information on how to use these Fabric OS v4.1 commands, refer to the appropriate *Fabric OS Reference Manual.*

For more information on Fabric OS commands relating to ISL Trunking, see Appendix A, *Commands Related to ISL Trunking.*

Table 3-1 ISL Trunking Telnet Commands for Fabric OS v4.1

Telnet Command	Description	Example
`portCfgTrunkport`	Enables or disables a port for ISL Trunking.	To enable a port, the following syntax is used: `portCfgTrunkPort <slotnumber> <portnumber>` The slot number only applies to ED-12000B. For example, to enable port 15 on a blade for the EMC ISL Trunking feature, enter: **`portCfgTrunkPort 2 15 1`** To disable port 15, enter: **`portCfgTrunkPort 2 15 0`**
`switchCfgTrunk`	Enables or disables trunking on all ports of a switch.	To enable EMC ISL Trunking on all ports of a switch, enter: **`switchCfgTrunk 1`** To disable EMC ISL Trunking on all ports of a switch, enter: **`switchCfgTrunk 0`**
`portCfgSpeed`	Sets the port speed to run at 2 GB.	To set the port speed to 2 GB, enter: **`portCfgSpeed x y 2`** where **`x`** is the slot number and **`y`** is the port number. The slot number only applies to ED-12000B.

Table 3-1 ISL Trunking Telnet Commands for Fabric OS v4.1 (*continued*)

Telnet Command	Description	Example
`switchCfgSpeed`	Sets the switch speed to auto negotiate.	To set the switch to auto negotiate, enter: **`switchCfgSpeed 0`**
`trunkshow`	Displays ISL Trunking membership information.	To display EMC ISL Trunking membership information about users, enter: **`trunkshow`**
`trunkdebug`	Displays trunk link failure	See *Troubleshooting* on page 3-14

Using Web Tools for ISL Trunking

Use Web Tools to view and modify ISL Trunking options through the **Trunk Information** tab and the **Port Settings** tab on the Switch Administration interface. For further information, refer to appropriate the *Web Tools User Guide*.

Use the **Web Tools Trunk Information** tab to view a summary of trunk groups and associated master and member ports. Table 3-2 describes the headings displayed from the Trunk Information tab.

Table 3-2 Trunk Information Tab Description

Trunk Information Tab	Description
Trunk Group	Displays a numerical number.
Master Port	Displays the associated master port for the group.
Member Ports	Shows the member ports associated with the group, separated by a comma.

Table 3-3 describes the headings and tasks performed using the EMC Web Tools **Port Setting** tab when Fabric OS is running (see Figure 3-1).

Table 3-3 Port Setting Tab Features

Port Setting Tab Features	Description
Port Number	Displays the port numbers.
Persistent Disable	Disables the selected port and maintains that state across power cycles, switch reboots, and switch disable/enable.
Enable Port	Enables a port.

Table 3-3 Port Setting Tab Features *(continued)*

Port Setting Tab Features	Description
Enable Trunking	Enables EMC ISL Trunking on a per port basis.
Port State	Gets port status, such as: online, offline, and no light.
Current Speed	Sets the speed of the port to 2 Gb/s.
Change Speed	Changes the port speed from 1 Gb/s to 2 Gb/s, or to the auto negotiate option.
Port Name	Displays the port name.

Important **ISL Trunking ports must always operate at 2 Gb/s. Setting the speed to 1 Gb/s prevents a port from participating in a trunk.**

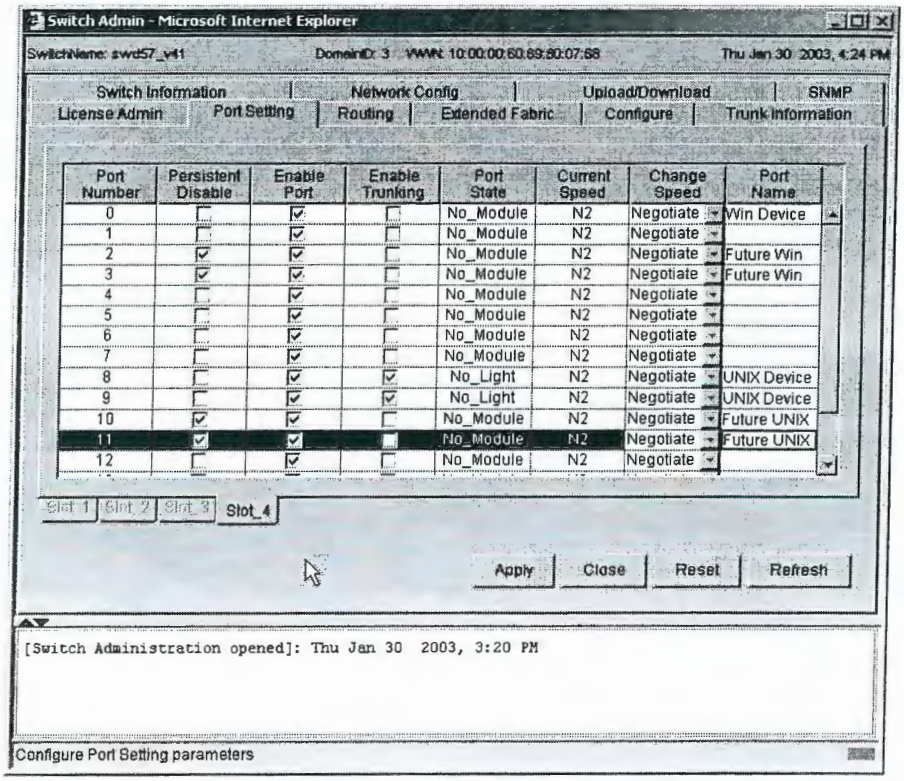


Figure 3-1 Port Setting Tab in the Switch Admin Window of Web Tools

Enabling and Disabling Trunking Through Web Tools

Web Tools can be used to enable and disable trunking.

To enable or disable trunking for one or more ports through Web Tools:

1. Launch Web Tools by launching the web browser and entering the switch name or IP address in the URL field.
2. Double-click to select the switch from the navigation tree.
3. Click the **Admin** button.
4. Log into the switch as admin.
5. Select the **Port Setting** tab.
6. Select or deselect the checkboxes in the **Trunking** column to enable or disable trunking for each port (deselect to disable trunking). See Figure 3-1.
7. Click **Apply.**

Trunking is immediately enabled or disabled for each port according to the selections.

Specifying Port Speeds

Port speeds can be set for the entire switch or for individual ports using either the CLI or Web Tools. If trunking is enabled, the only supported speeds are 2 Gb/s and auto-negotiate for ports that are being used for trunking. For ports that are not in a trunk, 1 Gb/s is also supported.

Setting Port Speeds Through the Command Line Interface

A telnet or serial session can be used to set the port speed for an individual port or the entire switch.

To specify the speed for all the ports on the switch using the CLI:

1. Open a CLI connection (telnet or serial) to the switch to be modified.
2. Log into the switch as admin.
3. Enter the following:

   switchcfgspeed speedlevel

   Speedlevel = Link speed, as follows:

0	Auto-negotiating mode. The port automatically configures for the highest speed.
1	Gb/s mode. The port will be at fixed speed of 1 Gb/s. This setting is not supported if trunking is enabled on the port.
2	Gb/s mode. The port will be at fixed speed of 2 Gb/s.

- Setting the speed for all ports on the switch to 2 Gb/s:

```
switch:admin> switchcfgspeed 2
Committing configuration...done.
switch:admin>
```

- Setting the speed for all ports on the switch to auto-negotiate:

```
switch:admin> switchcfgspeed 0
Committing configuration...done.
switch:admin>
```

To specify the speed for an individual port:

1. Open a CLI connection to the switch to be modified.
2. Log into the switch as admin.
3. Enter the following:

   portcfgspeed *slotnumber/portnumber speedlevel*

   slotnumber = Number of the switch slot; only required for the ED-12000B

   portnumber = Number of the port

   speedlevel = Speed of the link, as follows:

0	Auto-negotiating mode. The port automatically configures for the highest speed.
1	Gb/s mode. The port will be at fixed speed of 1 Gb/s. This setting is not supported if trunking is enabled on the port.
2	Gb/s mode. The port will be at fixed speed of 2 Gb/s.

- Setting the speed for port 3 on slot 2 to 2 Gb/s:

```
switch:admin> portcfgspeed 2/3 2

done.
switch:admin>
```

- Setting the speed for port 3 on slot 2 to auto-negotiate:

```
switch:admin> portcfgspeed 2/3 0

done.
switch:admin>
```

Setting Port Speeds Through Web Tools

Web Tools can be used to set the speed for one or more ports on a switch.

To specify the speed for one or more ports through Web Tools:

1. Launch Web Tools by launching the web browser and entering the switch name or IP address in the URL field.
2. Double-click to select the switch from the navigation tree.

3. Click the **Admin** button.
4. Log into the switch as admin.
5. Select the **Port Setting** tab.
6. Click the arrow in the **Change Speed** column and select the desired speed from the pull-down menu. See Figure 3-1.

   Trunking only supports speeds set to auto-negotiating and 2 Gb/s.

7. Click **Apply**.

   The ports are immediately set to the specified speeds.

Displaying Trunking Information

Web Tools or a telnet or serial session can be used to view information about the trunking groups that exist on the local switch.

Displaying Trunking Information Through the Command Line Interface

The `trunkshow` command can be used to display information about trunking groups. This command provides information in the following columns:

- Number of the trunking group.
- Port-to-port connections of the group, listed by port number (local port -> remote port).
- WWNs of the local ports in the group.
- Deskew values - the time difference for traffic to travel over each ISL as compared to the shortest ISL in the group. The number corresponds to nanoseconds divided by 10.
  The firmware automatically sets the minimum deskew value of the shortest ISL to 15.
- Whether the port is the master port for the trunking group.

To display trunking information through the CLI (telnet or serial session):

1. Open a CLI connection to the switch for which trunking information is desired.
2. Log into the switch as admin.
3. Enter the `trunkshow` command.

```
switch:admin> trunkshow

 1: 1 ->  1   10:00:00:60:69:04:10:83   deskew 16 Master
    0 ->  0   10:00:00:60:69:04:10:83   deskew 15

 2: 4 ->  4   10:00:00:60:69:04:01:94   deskew 16 Master
    5 ->  5   10:00:00:60:69:04:01:94   deskew 15
    7 ->  7   10:00:00:60:69:04:01:94   deskew 17
    6 ->  6   10:00:00:60:69:04:01:94   deskew 16

 3:14 -> 14   10:00:00:60:69:04:10:83   deskew 16 Master
   15 -> 15   10:00:00:60:69:04:10:83   deskew 15

switch:admin>
```

Displaying Trunking Information Through Web Tools

Web Tools lists each trunking group on the switch, with the master and subordinate ports for each group.

To display trunking information through Web Tools:

1. Launch the web browser and enter the switch name or IP address in the URL field.
2. Double-click to select the switch from the navigation tree.
3. Click the **Admin** button.
4. Log into the switch as admin.
5. Select the **Trunk Information** tab. See Figure 3-2.

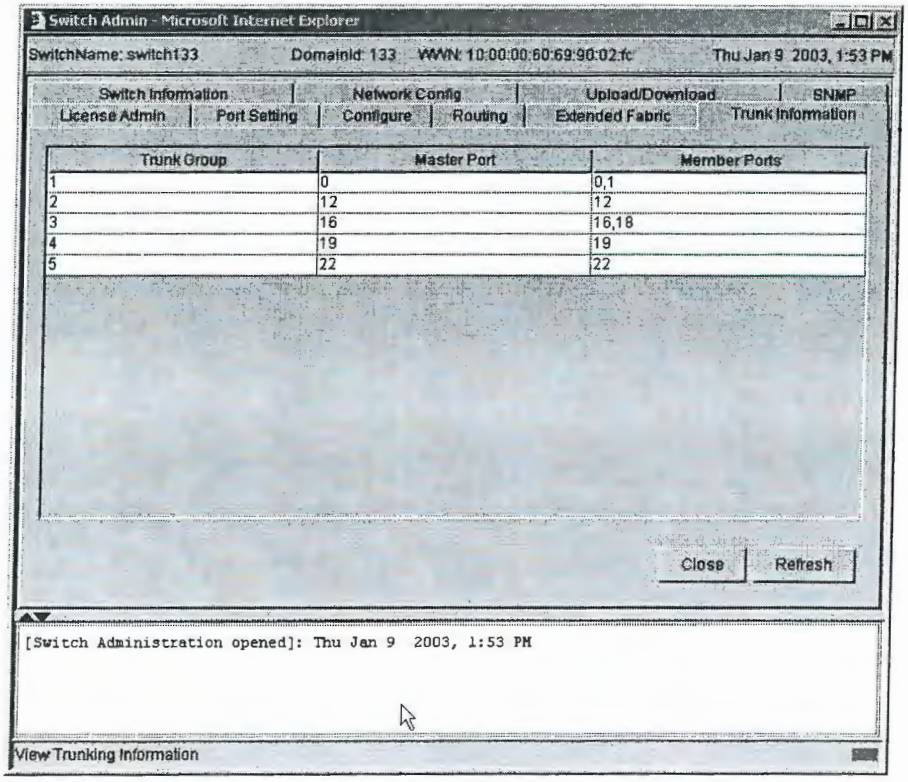


Figure 3-2 Trunk Information Tab in the Switch Admin Window of Web Tools

Troubleshooting

Troubleshooting information can be accessed through two methods: the `trunkdebug` command and the Error Log.

Debugging a Trunking ISL Failure

If a trunked ISL link fails debugging information is available through the CLI for use in troubleshooting and error correction.

To view debugging information for a trunking ISL failure:

1. Open a CLI connection to the switch to be modified.
2. Log into the switch as admin.
3. Enter the following:

   trunkdebug *AreaNumber1, AreaNumber2*

   AreaNumber1 = Area number of one of the ports in the trunking group

   AreaNumber2 = Area number of another of the ports in the trunking group.

Example

Viewing debug information for ports 3 and 5, where port 3 has not correctly configured as an E_Port:

```
switch:admin> trunkdebug 3 5
   port 3 is not E port
switch:admin>
```

The debug error messages are self-explanatory. For more information about this command, see *trunkdebug* on page A-8.

Interpreting ISL Trunking Error Messages

The two error messages that relate to ISL Trunking are described below. The error log can be accessed through the `errshow` and `errdump` commands.

Warning BLOOM-TRNK_MSTR_DWN...

This type of message indicates that the master ISL has been disconnected or has failed.

```
Warning BLOOM-TRNK_MSTR_DWN, 3, S3, P47: Trunk master
   port 47 goes OFFLINE in trunk group [47 46]
```

In this example,

- *"3"* indicates the severity level of the error (0 = panic, 1 = critical, 2 = error, 3 = warning, 4 = info, and 5 = debug).
- *"S3"* indicates the slot number.
- *"port 47"* indicates the area number of the master port.
- *"[47 46]"* indicates the ports that are participating in the trunking group.

Recommended Action:

1. If this error is displayed, determine whether the master ISL has been physically disconnected.
2. If the master ISL has not been disconnected, enter the `portlogdump` and `fabstateshow` commands, save the output, and contact EMC Technical Support for assistance.

Warning BLOOM-TRNK_SLV_DWN...

This type of message indicates that the subordinate ISL has been disconnected or has failed.

```
Warning BLOOM-TRNK_SLV_DWN, 3, S3, P46: Trunk slave port
   46 goes OFFLINE in trunk group [47 46]
```

In this example,

- *"3"* indicates the severity level of the error (0 = panic, 1 = critical, 2 = error, 3 = warning, 4 = info, and 5 = debug).
- *"S3"* indicates the slot number.
- *"port 46"* indicates the area number of the subordinate port.
- *"[47 46]"* indicates the ports that are participating in the trunking group.

Recommended Action:

1. If this error is displayed, determine whether a subordinate ISL has been physically disconnected.
2. If a subordinate ISL has not been disconnected, enter the `portlogdump` and `fabstateshow` commands, save the output, and contact EMC Technical Support for assistance.

Frequently Asked Questions About ISL Trunking

Table 3-4 lists frequently asked questions about ISL Trunking:

Table 3-4 Frequently Asked Questions About ISL Trunking

Frequently Asked Questions	Answers
Is the ISL Trunking feature automatically configured?	Yes. Following the purchase and installation of a license, the ISL Trunking feature is automatically invoked when ISLs are added between any two compatible switches as long as the ports are enabled for trunking.
Does ISL Trunking replace Dense Wavelength Division Multiplexing (DWDM)?	No. DWDM is a ring, and if a failure occurs it reroutes the allocated wavelength over alternate routes, and therefore changes the affected cable lengths.
What happens if an ISL in the trunk slave port fails?	If one of the trunk slave ports fails, the logical ISL stays up; however, its capacity is reduced by 2 Gb/s, and no route failure or re-routing of traffic occurs.
What happens if a trunk master fails?	If a trunk master fails, the logical ISL goes down, and FSPF perceives a momentary route failure. The trunk immediately re-forms without the failed ISL, and traffic resumes over the re-formed trunk with capacity reduced by 2 Gb/s. A new master port is assigned to form a logical ISL for routing.
Are trunks automatically established when the trunking feature is enabled?	Yes. When two, three, or four adjacent ISLs are connected to two switches, the switches automatically group the ISLs into a single logical ISL, or trunk.
Is it possible to have more than one trunk between a pair of switches?	Yes, but it may not be desirable to do so.
When using a pair of switches, is there a limit on the number of trunks I can have on one switch?	No.

Table 3-4 Frequently Asked Questions About ISL Trunking (*continued*)

Frequently Asked Questions	Answers
Is it possible to trunk between a switch and an edge device's host or storage?	No.
Should port statistics be the same across all participating ISLs within a trunk?	Not necessarily, it depends on the payload variations at the frame level. While optimal bandwidth use is the goal of the EMC ISL Trunking feature, traffic might not be distributed exactly the same across all ISLs within a trunk.
Is a trunking master the same as the principal ISL?	Not necessarily. A trunking master might be a principal ISL; however, a principal ISL can also exist when trunking is not enabled. A trunking master applies only when the trunking feature is enabled.
What is a trunking slave?	Non-master trunking ports from a trunking group are called slaves. The failure of any slave port has minimal impact on the traffic flow of a trunk.
What is a trunking link?	The components that make up a trunk are referred to as trunking links. A link consists of the two trunking ports and the connecting components: a small form-factor pluggable (SFP) and a cable. A trunking link is analogous to an ISL.
Which Extended Fabric Modes are supported?	"L0" mode, which is the default mode. If the ports in the potential trunking group use any other modes, the trunking group does not form.
Is trunking supported for 1 Gb/s?	No, trunking requires 2 Gb/s capacity.

A

Commands Related to ISL Trunking

This appendix includes the following information

Command List

Table A-1 provides summary information about the commands that relate to ISL Trunking.

Table A-1 Fabric OS Commands Related to ISL Trunking

Command	Function	Limitations
portcfgspeed	Use to specify the port speed.	Enter on the switch with the port to be configured.
portcfgtrunkport	Use to enable or disable trunking for a port.	Enter on the switch with the port to be configured.
switchcfgspeed	Use to set all ports of the switch to a particular speed.	Enter on the switch to specify port speeds.
switchcfgtrunk	Use to enable or disable trunking for all the ports of a switch.	Enter on the switch to enable or disable ISL Trunking.
trunkdebug	Use to debug a trunk link failure.	Enter on the switch to debug a trunk failure.
trunkshow	Use to display trunking information.	Enter on the switch to show ISL Trunking information.

portcfgspeed

Synopsis **portcfgspeed** *[slotnumber/]portnumber [speedlevel]*

Availability Admin

Description Use this command to specify the speed of a port to a particular level. After this command is issued, the port is disabled and enabled so that the port comes up with the new speed setting. The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

If the command is specified without an operand, you are prompted to enter the speed value.

The output of the `portshow` command displays the current achieved speed for the port, and the `portcfgshow` command displays the desired speed setting for the port.

Operands This command has the following operands:

slotnumber	Specify the number of the port card on which the port is located. This operand is optional.
portnumber	Specify the port number where you want to enable or disable trunking. This operand is required.
speedlevel	Specify the speed of a port. This operand is optional. Valid level values are one of the following:

0	Auto-negotiating mode. The port automatically configures for the highest speed.
1	Gb/s mode. The port will be at fixed speed of 1 Gb/s. This setting is not supported if trunking is enabled on the port.
2	Gb/s mode. The port will be at fixed speed of 2 Gb/s.

Example To specify the speed of port 3 on the port card in slot 2 to 2 Gb/s:

```
switch:admin> portcfgspeed 2/3 2
done.
```

See Also

```
switchcfgspeed
portshow
```

portcfgtrunkport

Synopsis **portcfgtrunkport** *[slotnumber/]portnumber [1|0]*

Availability Admin

Description Use this command to specify a port to be enabled or disabled for trunking.

This command requires the ISL Trunking license.

Operands This command has the following operands:

slotnumber	Specify the number of the port card on which the port is located. This operand is optional.
portnumber	Specify the port number where you want to enable or disable trunking. This operand is required.
1|0	Specify 1 to enable this port for trunking. Specify 0 to disable this port for trunking. This operand is required.

Example To enable trunking for port 3 of the port card in slot 1:

```
switch:admin> portcfgtrunkport 1/3 1
Committing configuration...done.
```

See Also
```
switchcfgtrunk
portshow
portcfgshow
switchshow
```

switchcfgspeed

Synopsis `switchcfgspeed [speedlevel]`

Availability Admin

Description Use this command to specify the speed of all the ports on a switch at a particular level. The configuration is saved in the non-volatile memory and persists across switch reboot or power cycle.

If the command is specified without an operand, you are prompted to enter the speed level value. An input of CTRL-D cancels the configuration update.

The output of `portshow` and `portcfgshow` displays the speed level:

- In the `portshow` output, the speed level is indicated as the current port speed of "1vGb/s" or "2vGb/s."
- In the `portcfgshow` output, the speed level is indicated as "1G", "2G", or "AN" (Auto-Negotiate).

Operands This command has the following operand:

speedlevel	Specify the speed of a port. This operand is optional. Valid values are one of the following:

0	Auto-negotiating mode. The port automatically configures for the highest speed.
1	Gb/s mode. The port will be at fixed speed of 1 Gb/s. This setting is not supported if trunking is enabled on the port.
2	Gb/s mode. The port will be at fixed speed of 2 Gb/s.

If the command is specified without an operand, you are prompted to enter a value.

Example To set the speed level for all ports on a switch to 2 Gb/sec:

```
switch:admin> switchcfgspeed 2
Committing configuration...done.
switch:admin>
```

See Also `portcfgspeed`
`switchshow`

switchcfgtrunk

Synopsis `switchcfgtrunk 0|1`

Availability Admin

Description Use this command to enable or disable trunking on all the ports of a switch.

This command requires the ISL Trunking license.

Operands This command has the following required operand:

1|0	Specify 1 to enable trunking on all the ports on this switch. Specify 0 to disable trunking on all the ports on this switch.

Example To enable trunking on a switch:

```
switch:admin> switchcfgtrunk 1
Committing configuration...done.
```

See Also

```
portcfgtrunkport
portshow
portcfgshow
switchshow
```

trunkdebug

Synopsis `trunkdebug` *AreaNumber1, AreaNumber2*

Availability Admin

Description Use this command to debug a trunk link failure. This command reports one of the following messages based on the trunking properties of the two specified ports:

- Switch doesn't support trunking
- Trunking license required
- Trunking is not supported in switch interop mode
- port<port_id> is not E_Port
- port<port_id> trunking disabled
- port<port_id> speed is not 2G
- port<port_id> and port<port_id> are not on same quad
- port<port_id> and port<port_id> connect to different switches
- port<port_id> is not trunking port due to: E_Port being disabled, or trunking may be disabled at remote port
- port<port_id> and port<port_id> can't trunk, please check ISL length to make sure difference is less than 400 meters

Operands This command has the following operands:

AreaNumber1	Specify the area number of port 1 (0-63). This operand is required.
AreaNumber2	Specify the area number of port 2 (0-63). This operand is required.

Area number is an alternate designation to *slot/port*; ports are numbered beginning with the bottom port in the left most slot (when facing the port side of the chassis), up each card then continuing at the bottom of the next card, and ending with the port at the top of the right most slot. For the ED-12000B, area numbers range from 0 to 63 for each logical switch; if a slot is empty, the numbers that would be assigned to that card are skipped.

Example To debug a trunk connection:

```
switch:admin> trunkdebug 43 44

Switch doesn't support trunking.
```

See Also

trunkshow
portcfgtrunkport
switchcfgtrunk

trunkshow

Synopsis `trunkshow`

Availability All users

Description Use this command to display trunking information. The fields displayed are as follows:

Trunking Group Number	Displays each trunking group on a switch. All the ports that are part of this trunking group are displayed.
Port-to-port connections	Displays the port to port trunking connections.
WWN	Displays the WWN of the connected port.
deskew	Displays the time difference for traffic to travel over the indicated ISL as compared to the shortest ISL in the group. The number corresponds to nanoseconds divided by 10. The firmware automatically sets the minimum deskew value of the shortest ISL to 15.
Master	Displays whether this trunking port connection is the master port connection for the trunking group.

Operands None

Example To display trunking information for a switch:

```
switch:admin> trunkshow
1: 1 ->  1   10:00:00:60:69:04:10:83   deskew 15 Master
   0 ->  0   10:00:00:60:69:04:10:83   deskew 15

2: 4 ->  4   10:00:00:60:69:04:01:94   deskew 16 Master
   5 ->  5   10:00:00:60:69:04:01:94   deskew 15
   7 ->  7   10:00:00:60:69:04:01:94   deskew 17
   6 ->  6   10:00:00:60:69:04:01:94   deskew 16
```

```
3:14 -> 14    10:00:00:60:69:04:10:83    deskew 16 Master
  15 -> 15    10:00:00:60:69:04:10:83    deskew 15
```

See Also

```
portcfgtrunkport
switchcfgtrunk
```

B

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure B-1).

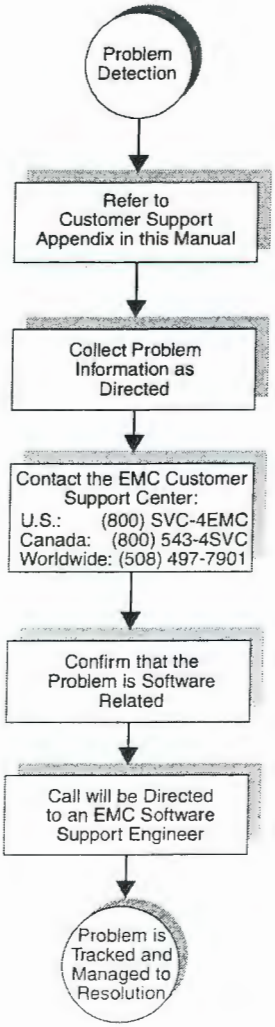


Figure B-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

http://powerlink.emc.com

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 withED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode*.

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit*.

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL*.

M

Media See *Transceiver*.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port*.

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

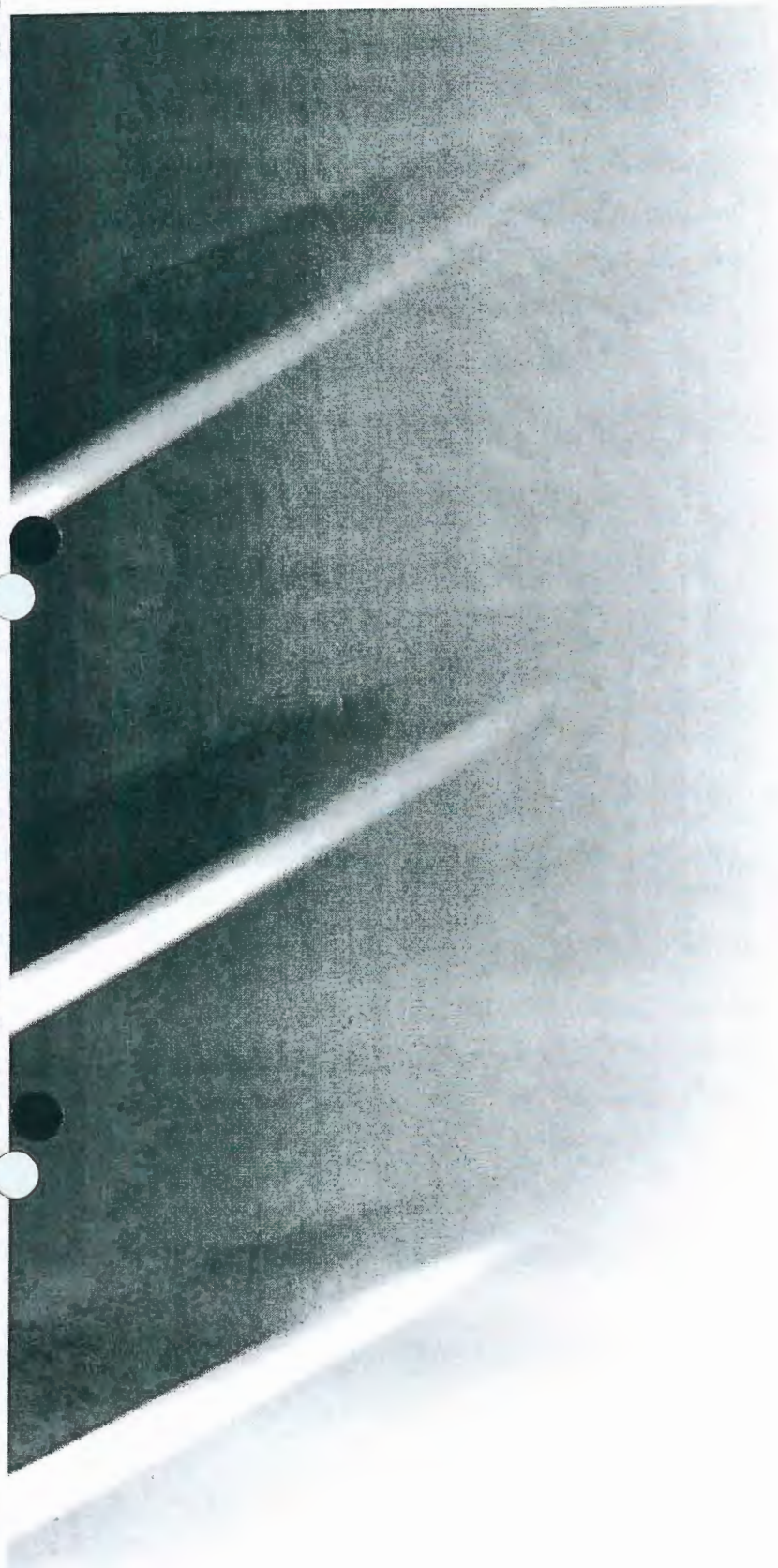
Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

Index

ANEXO SWITCH TIPO 03
PARTE 12

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br



EMC Connectrix B Series Performance Monitoring

Version 3.1 and Version 4.1

USER GUIDE

P/N 300-000-641
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

Connectrix B Series systems have been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

Trademark Information

Contents

Preface

The EMC Connectrix B Series Performance Monitoring User Guide provides information on Performance Monitoring that you may encounter during installation and operation of the DS-16B2, DS-32B2, and ED-12000B.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch and Enterprise Director. For the most up-to-date information on product features, see your product release notes.

If a feature in the DS-16B2, DS-32B2, or ED-12000B does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

This guide is part of the EMC Switch documentation set, and is intended for use by system administrators and others during installation and configuration of Performance Monitoring.

Readers of this guide are expected to be familiar with the EMC Connectrix Switch operating environment.

Organization

This guide provides the following information about Performance Monitoring:

- Chapter 1, *Introducing Performance Monitoring*, provides an overview of Performance Monitoring.
- Chapter 2, *Installing Performance Monitoring*, provides instructions for installing Performance Monitoring using Telnet commands.

- Chapter 3, *Using Performance Monitoring*, provides information about configuring and using the Performance Monitoring Telnet commands.
- Appendix A, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with EMC Connectrix Switches.
- The *Glossary* defines for terminology used in this manual.

Related Publications

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-16B2 QuickLoop Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*

- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this guide:

Palatino, bold	• Dialog box, button, icon, and menu items in procedures • Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	• New terms or unique word usage in text • Command line arguments when used in text • Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	User entry. For example: **`symmpoll -p`**
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.EMC.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.EMC.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to **`techpub_comments@EMC.com`** with your opinions of this guide.

1 Introducing Performance Monitoring

This chapter introduces Performance Monitoring features, and explains how to perform Performance Monitoring through Telnet and Web Tools.

This chapter following information:

Overview

Performance Monitoring is a comprehensive tool for monitoring the performance of networked storage resources. This tool helps reduce total cost of ownership and over-provisioning while enabling SAN performance tuning, reporting of service-level agreements, and greater administrator productivity.

Performance Monitoring provides SAN performance management through an end-to-end monitoring system that enables you to:

- Increase end-to-end visibility into the fabric
- Enable more accurate reporting for service-level agreements and charged access applications
- Improve performance tuning and resource optimization
- Reduce troubleshooting time
- Promote better capacity planning
- Increase productivity with preformatted and customizable screens and reports

Performance Monitoring is an optionally licensed product that runs on the DS-16B2, DS-32B2, and ED-12000B switches. If you have a fabric that includes DS-16B you can take advantage of the end-to-end performance monitoring features by installing a DS-16B2, DS-32B2 or ED-12000B switch anywhere in the path between the Source ID and the Destination ID.

You can administer performance monitoring through either Telnet commands or Web Tools. If you use Web Tools, a license must also be installed on the switch.

Features

Performance Monitoring:

- Measures the bandwidth consumed by individual routes (host target pairs)
- Provides device performance measurements by port, AL_PA, and LUN
- Reports Cyclic Redundancy Check (CRC) error measurement statistics
- Measures trunking performance
- Compares IP versus SCSI traffic on each port
- Includes a wide range of predefined reports
- Allows you to create customized user-defined reports

Terminology Used in this Document

Table 1-1 Advance Performance Monitoring Terminology

AL_PA	Arbitrated Loop Physical Address. An 8 bit value used to uniquely identify an individual port within a loop. A loop may have one or multiple AL_PAs.
SID	3-byte Source ID of the originator device, in the `0xDomainAreaALPA (0xDDAAPP)` format.
DID	3-byte Destination ID of the destination device, in the `0xDomainAreaALPA (0xDDAAPP)` format .
CRC	Cyclic redundancy check; an error detection method. The CRC is 32 bits in the frame, after the data field, and before the EOF (end of frame).
FILTER	A pattern of values in the frame header to be matched for the Fibre Channel frames being transmitted and received by the port.
MASK	A field made up of hexadecimal values that are used to include or exclude portions of a frame header for a possible match.

Performance Monitoring With Telnet Commands

Telnet commands provide three different types of performance monitoring:

- AL_PA monitoring
- End-to-end monitoring
- Filter-based monitoring

Refer to Chapter 3, *Using Performance Monitoring*, for detailed information on how to use the Telnet commands to monitor performance.

AL_PA Monitoring

AL_PA monitoring provides information regarding the number of CRC errors occurring in Fibre Channel frames in a loop configuration. AL_PA monitoring collects CRC error counts for each AL_PA attached to a specific port.

End-to-End Monitoring

End-to-end monitoring provides information regarding transaction performance between the transaction source (SID) and destination (DID) on a fabric or a loop. Up to eight SID-DID pairs per port can be specified. For each of the SID-DID pairs, the following information is available:

- CRC error count on the frames for the SID-DID pair
- Fibre channel words that have been transmitted through the port for the SID-DID pair
- Fibre channel words that have been received by the port for the SID-DID pair

Filter Based Monitoring

Filter-based monitoring provides information about a filter's hit count. All user-defined filters are matched for all FC frames being transmitted from a port. Note the following example:

```
{offset, value 0[, value 1, ..., value 3]}
 A                B
```

IPG-000021

In this example, `offset` (A) is the byte offset value in the header of the FC frame and `value 0[, value 1,..., value 3]` (B) is a user-defined value, or a set of user-defined values. At least one value must be specified (value 0), but you can specify up to four values.

For a filter to be matched, all the elements specified in the filter must provide a match.

For an element to produce a match, the value at offset (A) in the frame being transmitted must match at least one of the user-defined values (B).

The range of offsets that can be matched using filters is 0 to 63. Examples of FC frame statistics that can be measured using filters are:

- A filter consists of a set of elements in the following format: SCSI Read, Write, or Read/Write commands
- IP versus SCSI traffic comparison

In version 4.x when using End-to-End or Filter-based monitors you must specify a probing interval for the hardware counters that is a multiple of five seconds. EMC recommends that the probing interval be at least ten seconds. This requirement does not apply to version 3.x.

Performance Monitoring With Web Tools

You can monitor performance using Web Tools. The enhanced Performance Monitoring features in Web Tools provide:

- Predefined reports for AL_PA, end-to-end, and filter-based performance monitoring
- User-definable reports
- Performance canvas for application level or fabric level views
- Configuration editor (save, copy, edit, and remove multiple configurations)
- Persistent graphs across reboots (saves parameter data across reboots)
- Print capabilities

For more information on using Web Tools to administer Performance Monitoring, refer to Chapter 3, *Using Performance Monitoring*.

2 Installing Performance Monitoring

This chapter explains how to install Performance Monitoring.

This chapter provides the following information:

Overview

To enable Performance Monitoring, you must install a license on each switch that will use this feature. Contact EMC to obtain a license.

You can install a Performance Monitoring license through Telnet commands or through Web Tools.

Performance Monitoring is an optionally licensed product available on the EMC Connectrix Switches DS-16B2, DS-32B2 and Enterprise Director ED-12000B with any EMC qualified version of Fabric OS.

Installing Through Telnet

1. Log on to the switch using Telnet (refer to the appropriate *EMC Connectrix Fabric OS Procedures Manual* for details), using an account that has administrative privileges.
2. Type **licenseShow** on the Telnet command line to determine whether Performance Monitoring license is already installed on the switch.

   A list of all the licenses currently installed on the switch appears.

   The following example shows what the reader might see on a fully licensed switch.

Example

```
SB5_12000B_0:admin> licenseShow
RRRebbzzQSSSfcA:
    Fabric license
bbbdQRQ99mcceR4:
    Web license
    Zoning license
    Fabric Watch license
    Trunking license
R99ySdbb99WAAzTY:
    Extended Fabric license
    Performance Monitor license
SB5_12000B_0:admin>
```

3. If the Performance Monitoring license is not included in the list, continue with Step 4.
4. Enter the following on the command line:

   licenseAdd key

   where key is the license key exactly as provided by EMC. The license key is case sensitive and must be entered exactly as given.
5. Verify that the license was successfully added.

   Enter **licenseShow** on the command line:

Example

```
SB5_12000B_0:admin> licenseShow
RRRebbzzQSSSfcA:
    Fabric license
bbbdQRQ99mcceR4:
    Web license
    Zoning license
    Fabric Watch license
    Trunking license
```

```
R99ySdbb99WAAzTY:
    Extended Fabric license
    Performance Monitor license
SB5_12000B_0:admin>
```

Performance Monitoring features are available as soon as the license is added.

Installing Through Web Tools

You can install a license through Web Tools if a Web Tools license is already installed.

1. Launch a web browser.
2. Enter the switch name or IP address in the **Location/Address** field of the browser.
3. Press ENTER.

   Web Tools launches, displaying the Fabric View (refer to Figure 2-1).

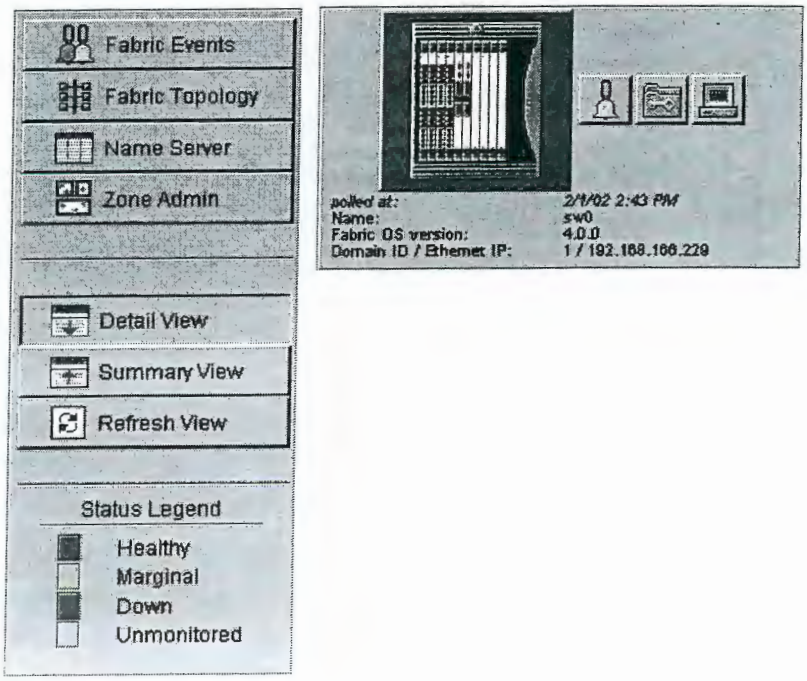


Figure 2-1 Fabric View

4. Click the **Admin** icon or the appropriate switch panel.

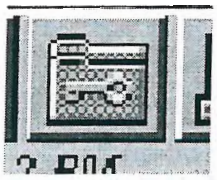


Figure 2-2 Web Tools Admin Icon

The logon window displays.

5. Enter a logon name and password with administrative privileges and press ENTER. The default administrator account name is `admin`.

   The Administration View appears.

6. Click the **License Admin** tab.

7. Enter the license key in the **License Key** field exactly as provided by EMC, and click **ADD** (refer to Figure 2-3).

Performance Monitoring features are available as soon as the license is added.

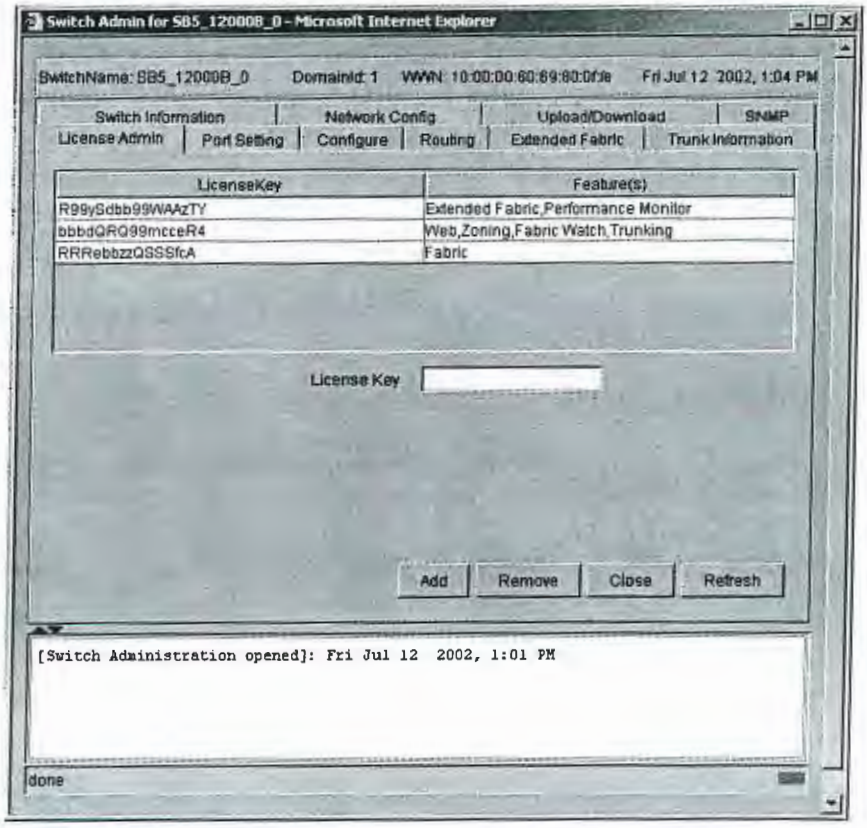


Figure 2-3 License Admin Tab

For more information about Web Tools, see the *EMC Connectrix B Series Web Tools User Guide.*

3 Using Performance Monitoring

You can administer Performance Monitoring through Telnet commands or through Web Tools, an optionally licensed product. This chapter describes performance monitoring through Telnet commands. It also shows how you can monitor changes made through Telnet by using Web Tools.

Overview

Telnet commands let you configure Performance Monitoring. The features in Web Tools, an optional product, let you see graphs of the performance of the switch.

For further information about performance monitoring through Web Tools, refer to the *appropriate Web Tools User Guide*.

Web Tools

You can monitor switch performance in the Performance View of Web Tools.

To access Performance Monitor through Web Tools follow these steps:

1. Launch Web Tools. The Fabric View appears.
2. Click the **Switch** icon of the switch you want to monitor, launching the Switch View, refer to Figure 3-1 on page 3-3.
3. Click on the **Perf** icon in the Switch View, launching the Performance Monitor window, refer to Figure 3-2 on page 3-4.

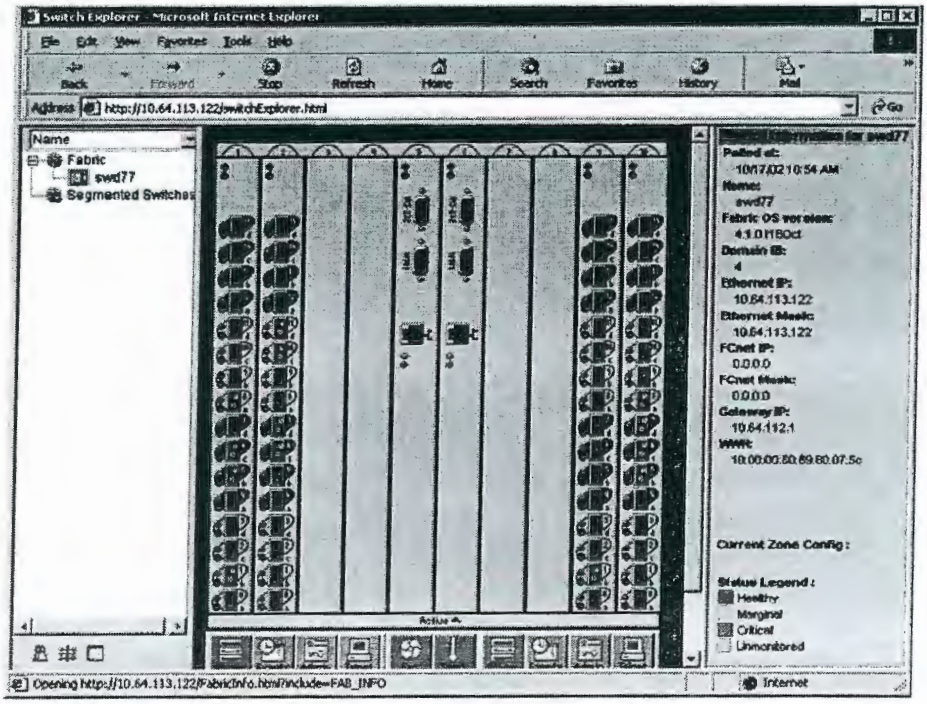


Figure 3-1 Switch View in Web Tools

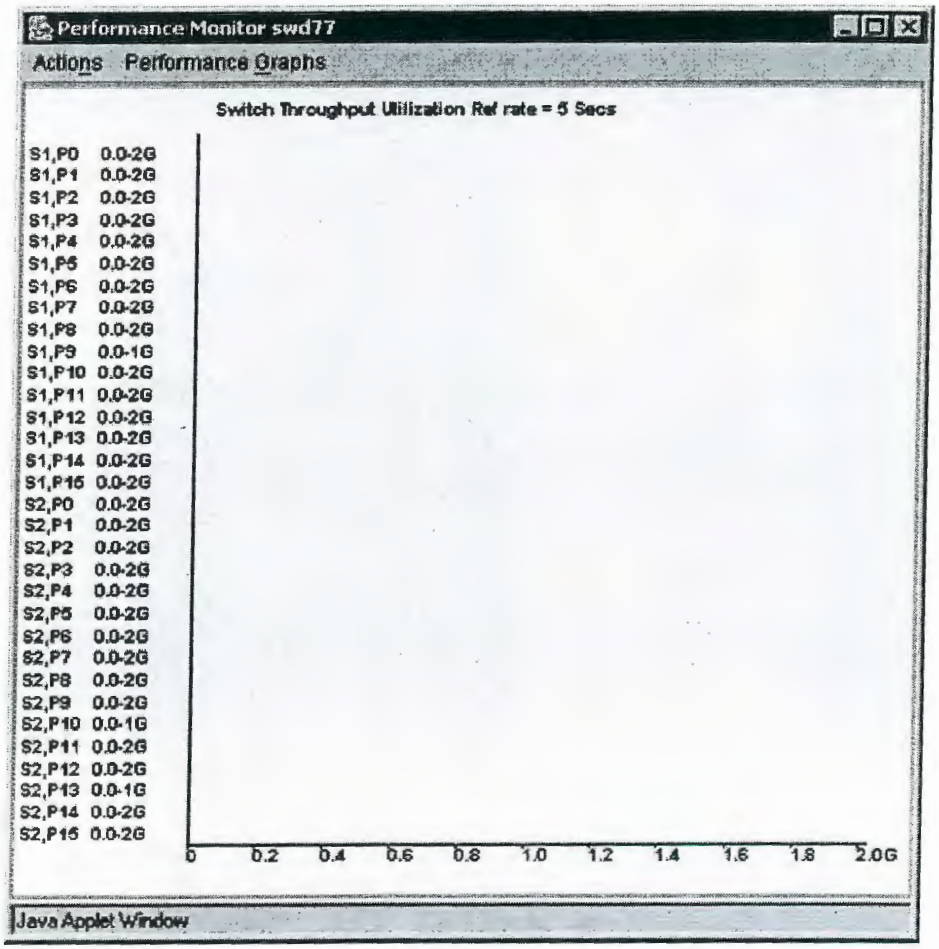


Figure 3-2 Performance Monitor

Predefined Performance Graphs

Predefined graphs are provided to simplify performance monitoring. A wide range of end-to-end fabric, LUN, device, and port metrics are included. Table 3-1 lists the predefined performance graphs available with both basic and performance monitoring. Figure 3-3 on page 3-6 shows how to access the list of predefined performance monitoring graphs in Web Tools.

Table 3-1 Predefined Performance Graphs

Basic Monitoring	Displays
Port Throughput	Performance of a port based in four-byte frames received and transmitted.
Switch Aggregate Throughput	Aggregate performance of all ports of a switch.
Switch Throughput Utilization	The port throughput at the time the sample is taken.
Port Error	A line of CRC errors for a given port.
Switch Percent Utilization	Percentage of usage of a chosen switch at the time the sample is taken.
Port Snapshot Error	CRC error count between sampling periods for all the ports on a switch.
Advanced Monitoring[a]	
SID/DID Performance	Traffic between a SID (or WWN) and a DID (or WWN) pair on the switch being managed.
SCSI vs. IP Traffic	Percentage of SCSI versus IP frame traffic on each individual port.
AL_PA Errors	CRC errors for a given port and a given AL_PA.
SCSI Commands by port and LUN (R, W, R/W)	Total number of read/write commands on a given port to a specific LUN.

a. These graphs are available only when a Performance Monitoring license is installed.

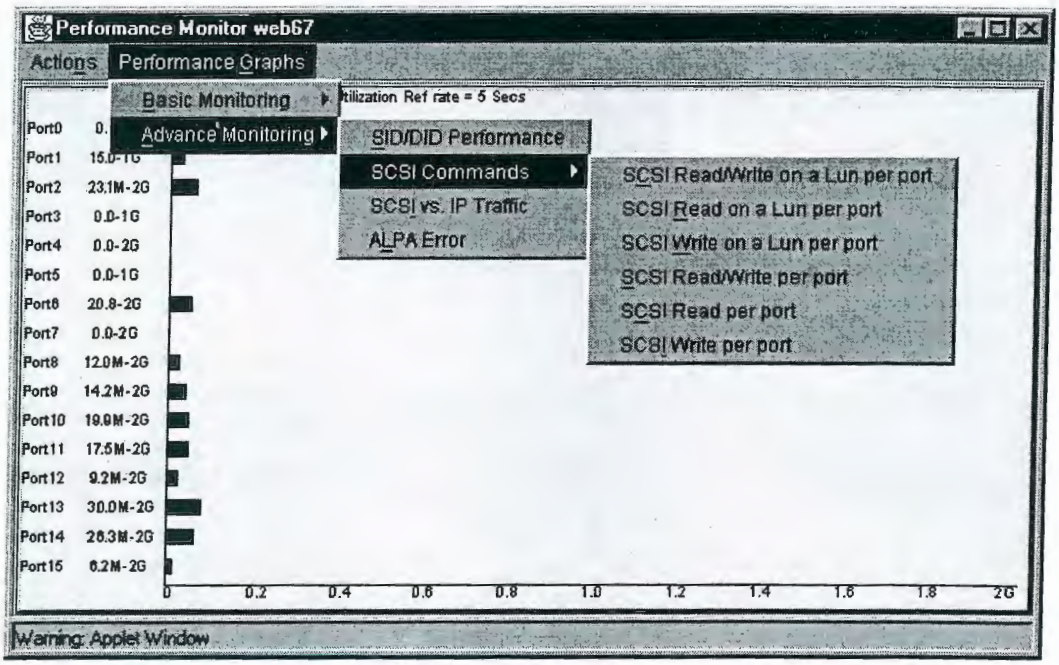


Figure 3-3 Accessing Predefined Performance Graphs

User-Defined Graphs

The predefined graphs can be modified based on parameter fields such as SID/DID, LUN, AL_PA, and port. These new user-defined graphs can be added and saved to canvas configurations.

Figure 3-4 shows a list of user-defined graphs defined in a canvas.

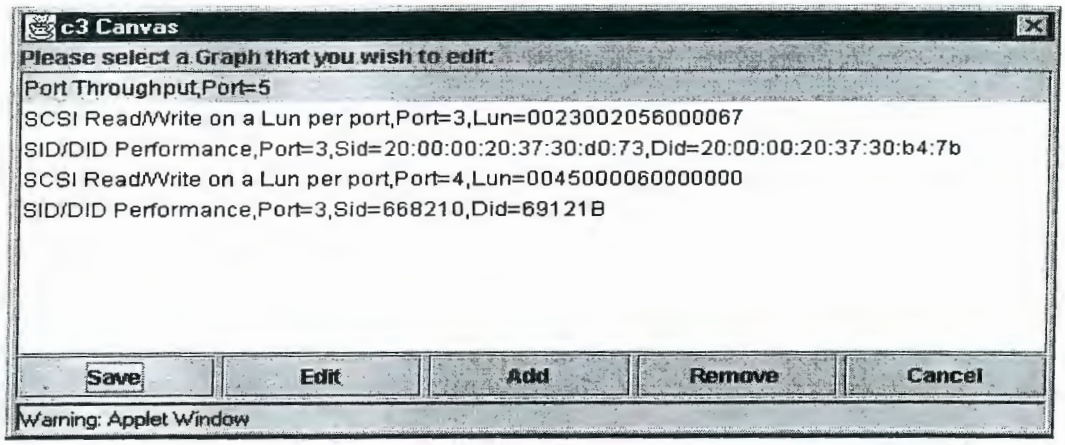
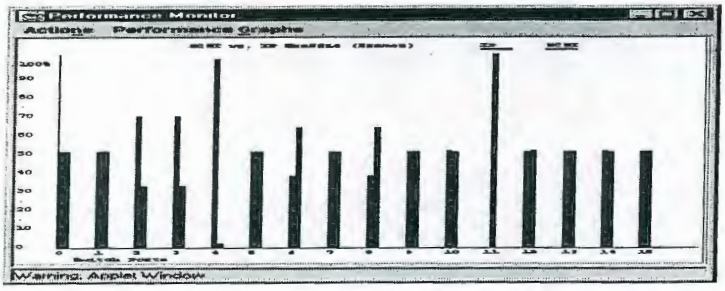


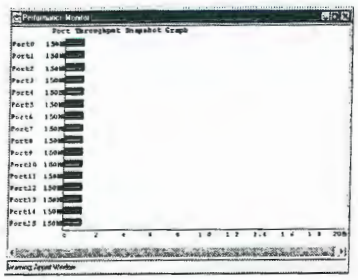
Figure 3-4 User-Defined Graphs

Performance Graph Formats

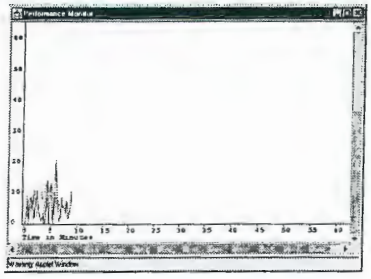
You can display performance graphs as vertical bar charts, horizontal bar charts, and line charts, as shown in Figure 3-5.



Vertical Bar Charts



Horizontal Bar Charts



Line Charts

Figure 3-5 Types of Performance Graphs

In addition to Figure 3-1, Figure 3-2, and Figure 3-3, the Performance Monitoring Resource Usage Display shown in Figure 3-6 shows which filter slots have been used for each port, and which are available. The color-coded interface makes troubleshooting easier.

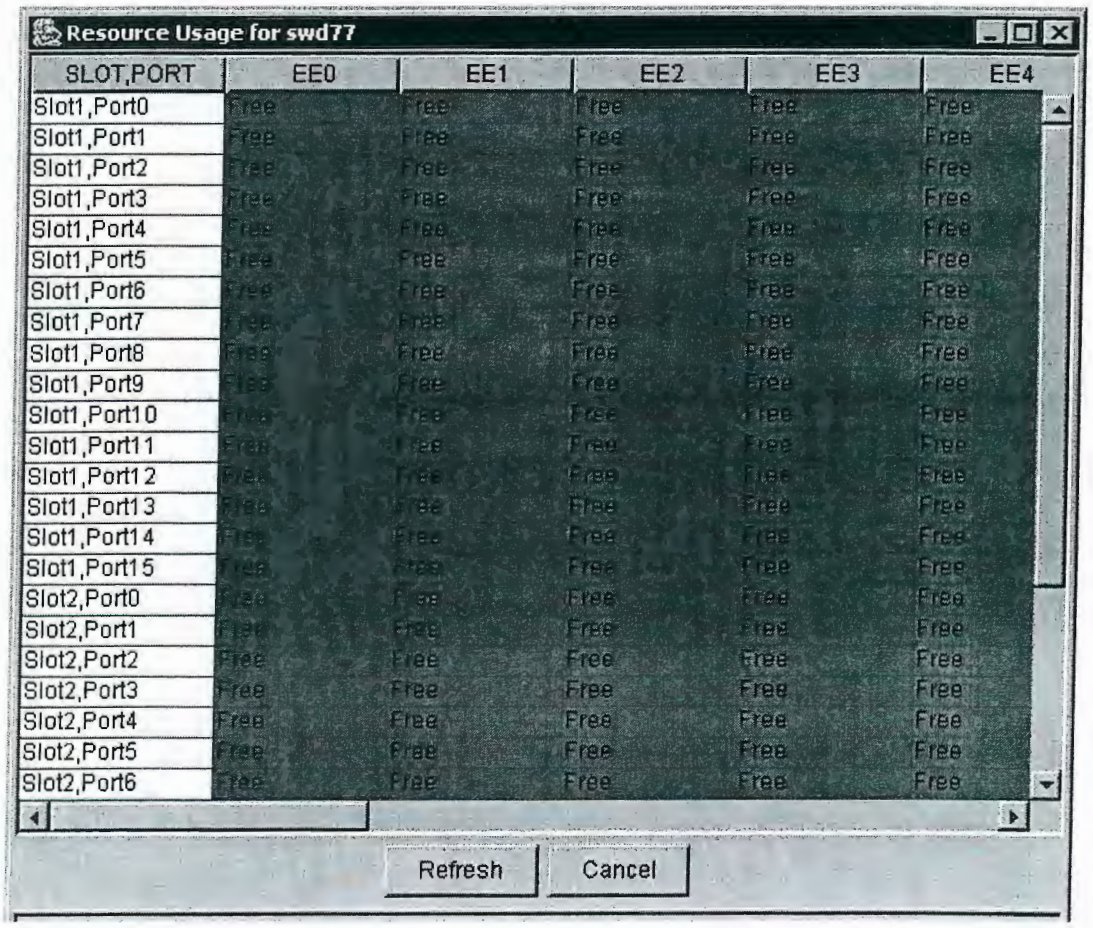


Figure 3-6 Performance Monitoring Resource Usage Display

For the ED-12000B, the port column also includes a slot number reference.

Performance Graph Canvas

The enhanced performance monitoring in Web Tools enables you to set up a canvas of performance graphs. The canvas can hold up to eight graphs per window, as shown in Figure 3-7.

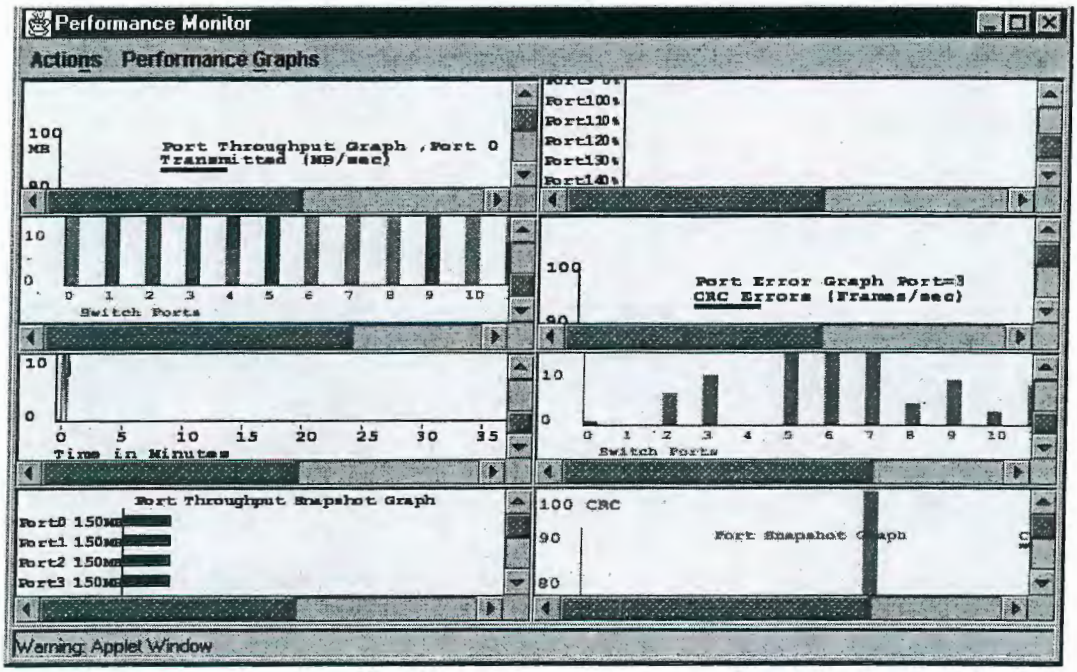


Figure 3-7 Canvas of Eight Performance Monitoring Graphs

Multiple canvases can be created for different users or different scenarios.

Adding Graphs to a Canvas

You can add graphs to a canvas by using the Performance Graphs menu on the Performance Monitor window. Select the graph you want to add to the canvas from either the Basic or Advanced Monitoring submenus. For a description of each of the graphs available, refer to Table 3-1 on page 3-5.

You can then use the Actions menu on the Performance Monitor window to:

- Save current canvas configuration
- Display canvas configuration
- Display current canvas configuration

- Print all graphs

For a detailed description of the options available in the Actions menu, refer to the *EMC Connectrix B Series Web Tools User Guide.*

Saving Canvas Configurations

You can save up to 20 individual canvases, each with up to eight graphs each. Save each canvas with a name, and an optional brief description.

To save a current canvas configuration:

1. Select the **Actions** menu on the Performance Monitor window.
2. Select **Save Current Canvas Configuration**. Figure 3-8 shows an example of saved canvases.

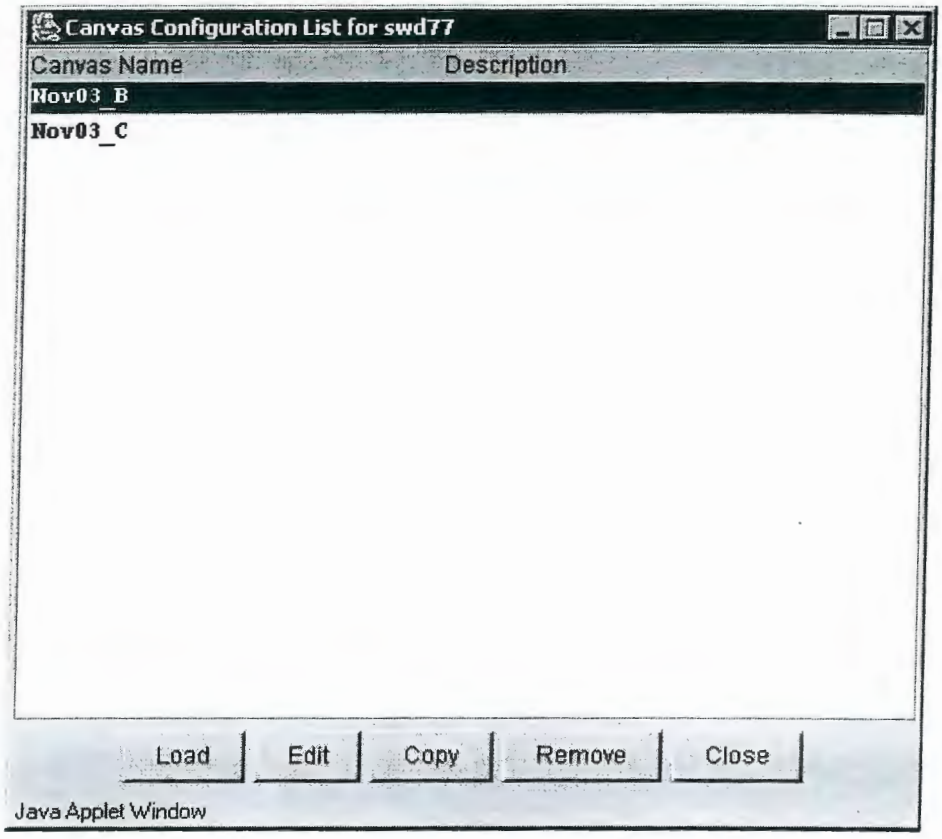


Figure 3-8 Saved Canvas Configuration

Printing All Graphs on a Configuration

You can print all the graphs on a selected canvas. Select the **Print All Graphs** option from the Actions menu on the Performance Monitor window. Select print options such as printer choice, print to file, and number of pages to print.

Telnet Commands

The Telnet commands for Performance Monitoring become available through the shell admin account when the Performance Monitoring license key is installed. To use a Telnet command, log in to the relevant switch with administrative privileges, enter the command along with any required arguments, and press ENTER.

Using Telnet commands, you can track the following:

- Number of CRC errors for AL_PA devices
- Number of words received and transmitted in fibre channel frames with a defined SID-DID pair
- Number of CRC errors in fibre channel frames with a defined SID/DID pair
- Number of times a particular command or frame type is received by a port

For a description of all the Telnet commands provided for performance monitoring, see the *EMC Connectrix Fabric OS Reference.*

Port Addressing and Area Numbering

The concept of area numbering is new for the ED-12000B. The area number is used in the same way a port number is used for the switches.

AL_PA Performance Monitoring

AL_PA performance monitoring allows you to track and display the number of CRC errors that have occurred on frames sent to each AL_PA on a specific port. AL_PA-based performance monitoring does not require explicit configuration. The switch hardware and firmware automatically monitors CRC errors for all valid AL_PAs.

Displaying the CRC Error Count

Use `perfShowAlpaCrc` to display the CRC error count for all AL_PA devices or a single AL_PA on a specific port. The port must be an active L_Port.

Example This command displays the CRC error count for all AL_PA devices on port 3:

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfShowAlpaCrc 3
```

```
AL_PA     CRC count
   --------------------

 0x01   2

 0x02   0

 0x04   1
```

Example The following command displays the CRC error count for AL_PA 0x01 on port 3:

```
sw1:admin> perfShowAlpaCrc 3, 0x01
The CRC count at ALPA 0x1 on port 3 is 0x000000002.
```

On an ED-12000B, the command is `perfShowAlpaCrc` slot number/port number, ALPA.

Clearing the CRC Error Count

Use `perfClrAlpaCrc` to clear the CRC error count for AL_PA devices on a specific port. You can clear the error counts for all the AL_PA devices on a port or for a specific AL_PA.

Example The following command clears the CRC error count for all AL_PA devices on port 3:

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfClrAlpaCrc 3
No ALPHA value is specified.
This will clear all ALPA CRC counts on port 3.
Do you want to continue? [y|n]y
Please wait ...
All alpa CRC counts are cleared on port 3.
```

On an ED-12000B, the command is `perfClrAlpaCrc` slot number/port number, ALPA.

Example The following command clears the CRC error count for AL_PA 1 on port 3:

```
admin> perfClrAlpaCrc 3, 0x01
CRC error count at ALPA 0x1 on port 3 is cleared.
```

End-to-End Performance Monitoring

End-to-end performance monitoring counts the number of words and CRC errors in fibre channel frames for a specified Source ID (SID) and Destination ID (DID) pair. An end-to-end performance monitor counts:

- Number of words in frames received at the port (RX_COUNT)
- Number of words in frames transmitted from the port (TX_COUNT)
- Number of CRC errors in frames received at the port (CRC_COUNT)

To enable end-to-end performance monitoring, you must configure an end-to-end monitor on a port, specifying the SID-DID pair. The monitor counts only those frames with matching SID and DID.

Each SID or DID has three fields, listed in the following order:

- Domain ID (DD)
- Area ID (AA)
- AL_PA (PP)

For example, the SID 0x118a0f has Domain ID 0x11, Area ID 0x8a, and AL_PA 0x0f. (The prefix 0x denotes a hexadecimal number.)

Adding End-to-End Monitors

Use `perfAddEEMonitor` to add an end-to-end monitor to a port. The monitor counts the number of words received, number of words transmitted, and number of CRC errors detected in frames qualified using either of following two conditions:

1. For frames received at the port (with End-to-End monitor installed) the frame SID is the same as "SourceID" and frame DID is the same as "DestID". Both RX_COUNT and CRC_COUNT will be updated accordingly.
2. For frames transmitted from the port (with End-to-End monitor installed) the frame DID is the same as "SourceID" and frame SID is the same as "DestID", TX_COUNT, and CRC_COUNT will be updated accordingly.

Use `perfAddEEMonitor` to specify the port, the SID, and the DID that you want to monitor. Depending on the application, you can select any port along the routing path for monitoring.

Example Figure 3-9 shows two devices:

- Host A, which is connected to domain 5, switch area port 12 (AL_PA 0x00) on switch X
- Dev B, which is connected to domain 11, switch area port 30 (AL_PA 0xef) on switch Y.

For the ED-12000B, a slot number and port number is needed.

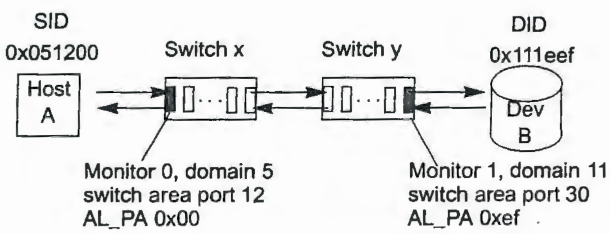


Figure 3-9 Setting End-to-End Monitors On a Port

To monitor the traffic from Host A to Dev B:

Add a monitor to port 12, specifying `0x051200` as the SID and `0x111eef` as the DID.

```
switch:admin> perfAddEEMonitor 12, "0x051200" "0x111eef"
end-to-end monitor number 0 added.
```

For the ED-12000B, the command would be `perfAddEEMonitor` slot number/port number, SID, DID.

To monitor the traffic from Dev B to Host A:

Add a monitor to port 14, specifying `0x111eef` as the SID and `0x051200` as the DID. Use the following commands:

```
switch:admin> perfAddEEMonitor 14, "0x111eef" "0x051200"
    end-to-end monitor number 1 added.
```

For the ED-12000B, the command would be `perfAddEEMonitor` slot number/port number, SID, DID.

Monitor 0 counts the frames that have an SID of 0x051200 and a DID of 0x111eef. For monitor 0, RX_COUNT is the number of words from Host A to Dev B, CRC_COUNT is the number of frames from Host A to Dev B with CRC errors, and TX_COUNT is the number of words from Dev B to Host A.

Monitor 1 counts the frames that have an SID of 0x111eef and a DID of 0x051200. For monitor 1, RX_COUNT is the number of words from Dev B to Host A, CRC_COUNT is the number of frames from Dev B to Host A with CRC errors, and TX_COUNT is the number of words from Host A to Dev B.

End-to-end performance monitoring monitors traffic on the receiving port respective to the SID only. In Figure 3-9 on page 3-15, if you add a monitor to port 2, specifying Dev B as the SID and Host A as the DID, no counters other than CRC are incremented.

```
Valid:     perfAddEEMonitor    2,  0x051200,   0x111eef
Notvalid:  perfAddEEMonitor    2,  0x111eef,   0x051200
```

Figure 3-10 on page 3-16 shows several switches and the proper ports on which to add performance monitors for a specified SID-DID pair.

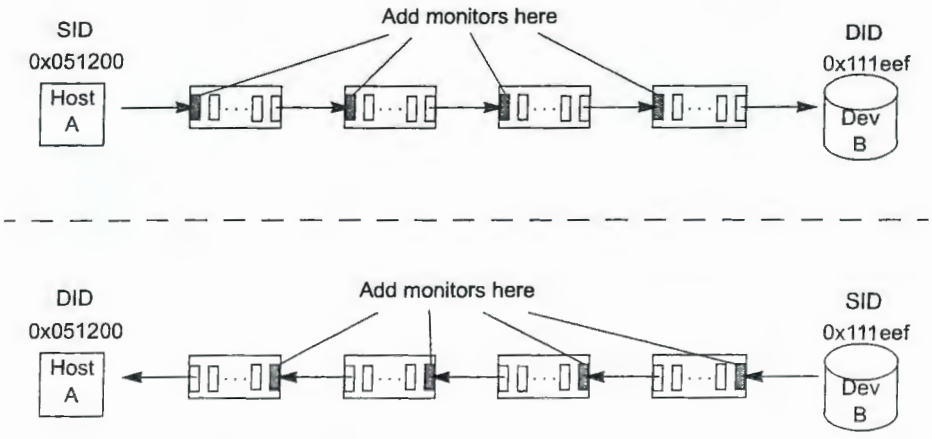


Figure 3-10 Proper Placement of End-to-End Performance Monitors

Setting a Mask for End-to-End Monitors

End-to-end monitors count the number of words in fibre channel frames that match a specific SID/DID pair. If you want to match only part of the SID or DID, you can set a mask on the port to compare only certain parts of the SID or DID. With no mask set, the frame must match the entire SID or DID to trigger the monitor counter. By setting a mask, you can choose to have the frame match only one or two of the three fields (Domain ID, Area ID, AL_PA) to trigger the monitor.

You can set only one mask per port. The mask is applied to all of the end-to-end monitors on a port. If you subsequently create new monitors on the port, the mask is applied to these new monitors as well. The counters are reset when you set the mask.

The mask is specified in the form dd:aa:pp where dd is the Domain ID mask, aa is the Area ID mask, and pp is the AL_PA mask. The values for dd, aa, and pp are either ff (the field must match) or 00 (the field is ignored).

Use `perfSetPortEEMask` to set a mask for end-to-end monitors. The command sets the mask for all end-to-end monitors of a port, so that you can selectively choose the Fibre Channel frames in which the number of words are to be counted.

If any end-to-end monitors are programmed on a port when you issue the `perfsetporteemask` command, you will see this message:

```
< n > EE monitors are currently programmed on this port.
   Changing EE mask for this port will cause ALL EE
   monitors on this port to be deleted. Do you want to
   continue? (yes, y, no, n): [no]

EE mask on port <port-number> is set and EE monitors were
   deleted
```

`perfSetPortEEMask` sets a mask for the Domain ID, Area ID, and AL_PA of the SIDs and DIDs for frames transmitted from and received by the port. Figure 3-11 on page 3-18 shows the mask positions in the command.

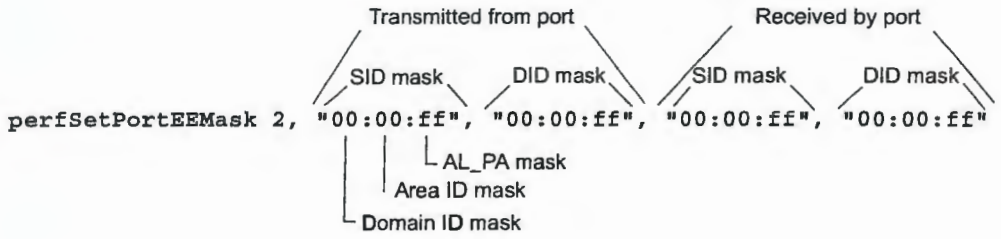


Figure 3-11 Mask Positions for End-to-End Monitors

In Figure 3-11, a mask `ff` is set on port 2 to compare the AL_PA fields on the SID and DID in all frames (transmitted and received) on port 2. The frame SID and DID must match only the AL_PA portion of the specified SID-DID pair. The Domain ID and Area ID fields in all frames are ignored, as no mask is set on these fields.

Example **To set the following monitor on a port:**

For the ED-12000B, a slot number and port number is needed.

```
perfAddEEMonitor 2, 0x051200, 0x111eef
```

then the frame SID must be `0x051200` and the frame DID must be `0x111eef` to trigger the monitor.

If you set the mask shown in Figure 3-11, then the frame SID and DID must match only the AL_PA portion of the specified SID-DID pair. That is, frames with SID of `0xnnnn00` and DID of `0xnnnnef` trigger the monitor, where nnnn is any number.

Each port can have only one EE mask. The mask is applied to all end-to-end monitors on the port. You cannot specify individual masks for each monitor on the port. If you define a new end-to-end monitor on a port after you have created a mask for that port, the mask is automatically applied to the new monitor.

The default EE mask value upon power on is `ff:ff:ff` for everything—SID and DID on all transmitted and received frames.

Example The following commands add an end-to-end monitor to port 2, and then set a mask on the SID and DID Domain ID of frames transmitted from port 2. After the mask is set, monitor `0` counts the number of words in incoming fibre channel frames that have a SID of `0x05nnnn` and DID of `0x11nnnn`, where nnnn is any number.

```
sw1:admin> perfAddEEMonitor 2, 0x051200 , 0x1l1eef
    end-to-end monitor number 0 added.
sw1:admin> perfSetPortEEMask 2, 00:00:00 , 00:00:00 ,
ff:00:00 , ff:00:00
   The EE mask on port 2 is set and EE counters are reset.
```

Displaying the End-to-End Mask of a Port

Use `perfShowPortEEMask` to display the current end-to-end mask of a port.

The end-to-end mask has 12 fields, with each field having a value of on or off.

Example The following commands set an end-to-end mask on port 11 and display the mask:

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfSetPortEEMask 11, 00:00:ff , 00:00:ff , 00:00:ff , 00:00:ff
   The EE mask on port 11 is set and EE counters are reset.
sw1:admin> perfShowPortEEMask 11
   The EE mask on port 11 is set by application  Telnet
   TxSID Domain:  off
   TxSID Area:    off
   TxSID ALPA:    on
   TxDID Domain:  off
   TxDID Area:    off
   TxDID ALPA:    on
   RxSID Domain:  off
   RxSID Area:    off
   RxSID ALPA:    on
   RxDID Domain:  off
   RxDID Area:    off
   RxDID ALPA:    on
```

Displaying End-to-End Monitors

Use `perfShowEEMonitor` to display all the end-to-end monitors defined on a port. You can display cumulative counters or a rolling table of counters at specified intervals. This command displays the following information on all end-to-end monitors:

- Monitor number (KEY)
- SID
- DID
- CRC error count (CRC_COUNT)
- Number of fibre channel words transmitted (TX_COUNT)
- Number of fibre channel words received (RX_COUNT)
- Creator application (OWNER_APP)
- IP address of the creator, if known (OWNER_IP_ADDR)

If you specify an interval number in `perfShowEEMonitor`, the command displays a rolling table of CRC error, Tx, and Rx counters on a per interval basis for all the valid monitors on the port. The counter values are the number of bytes, in decimal format.

If you omit the interval number, the command displays the cumulative transmit counter (TX_COUNT), receive counter (RX_COUNT), and CRC error counter. These cumulative counters are 64 bit values in hexadecimal format.

The minimum interval value that can be specified is 5 seconds.

Example The following command displays all of the end-to-end monitors on port 3 at an interval of six seconds. (In this example, there are three monitors on port 3, numbered 0, 1, and 2.)

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfShowEEMonitor 3, 6
   perfShowEEMonitor 3, 6: Tx/Rx are # of bytes and crc is
   # of crc errors

        0                1                2
------------  ------------  ------------
crc   Tx    Rx  crc   Tx    Rx  crc   Tx    Rx
============  ============  ============
 0    0     0   0    0     0    0    0     0
 0   53m 4.9m   0   53m 4.9m    0   53m 4.9m
 0   53m 4.4m   0   53m 4.4m    0   53m 4.4m
 0   53m 4.8m   0   53m 4.8m    0   53m 4.8m
 0   53m 4.6m   0   53m 4.6m    0   53m 4.6m
 0   53m 5.0m   0   53m 5.0m    0   53m 5.0m
 0   52m 4.6m   0   52m 4.6m    0   52m 4.6m
```

In the example above, "m" stands for megabytes. You may also see "g" which stands for gigabytes, or "k" which stands for kilobytes.

Example The following command displays the cumulative counters on all end-to-end monitors defined on port 3. The KEY column contains the monitor number.

```
switch:admin> perfShowEEMonitor 3
There are 3 end-to-end monitor(s) defined on port 3.

KEY  SID       DID       OWNER_APP  OWNER_IP_ADDR     TX_COUNT           RX_COUNT           CRC_COUNT
-------------------------------------------------------------------------------------------------------
0   0xb1300   0xb23ef   TELNET        N/A       0x00000004d0ba9915 0x0000000067229e65 0x0000000000000000
1   0xb1200   0xb22ef   TELNET        N/A       0x00000004d0baa754 0x0000000067229e87 0x0000000000000000
2    0x58e0f   0x1182ef Web_Tools192.168.169.40 0x00000004d0bade54  0x0000000067229e87 0x0000000000000000
```

Deleting End-to-End Monitors

Use `perfDelEEMonitor` to delete an end-to-end monitor on a port. Indicate which monitor to delete by specifying the monitor number that was returned by a previous `perfAddEEMonitor` command.

If you do not specify a monitor number, then all end-to-end monitors on the port are deleted.

Example The following command deletes the end-to-end monitor number 0 on port 2:

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfDelEEMonitor 2, 0
end-to-end monitor number 0 deleted
```

Example The following command deletes all of the end-to-end monitors on port 2:

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfDelEEMonitor 2
This will remove ALL EE monitors on port 2, continue?
   [y|n]y
```

Clearing End-to-End Monitor Counters

Use the `perfcleareemonitor` command to clear statistics counters for all or a specified end-to-end monitor on a port. After the command has been executed, the telnet shell confirms that the monitor counters have been cleared. Before issuing this command, verify that all of the valid end-to-end monitor numbers on a specific port using the `perfshoweemonitor` command to make sure the correct monitor counters will be cleared. The example clears statistic counters for an end-to-end monitor on slot 1, port 2, monitor 5.

In 4.1 and 3.1 issuing the command `portStatsClear` on a port will also result in all End-to-End monitors being cleared for all the ports in the same quad.

Example

```
switch:admin> perfcleareemonitor 2, 5
End-to-End monitor number 5 counters are cleared
```

For the ED-12000B, a slot number and port number is needed.

Filter-Based Performance Monitoring

Filter-based monitoring counts the number of times a particular command or frame type is received by a port. Filter-based monitoring is achieved by configuring a filter for a particular purpose. The filter can be a standard filter (for example, a read command filter that counts the number of read commands that have been received by the port) or a user-defined filter that you customize for your particular use.

The maximum number of filters is eight per port, in any combination of standard filters and user-defined filters.

Adding Standard Filter-Based Monitors

This section describes how to add standard filter-based monitors to a port. Use the Telnet commands listed in the following table to define filter-based monitors on a port.

Table 3-2 Telnet Commands to Add Filter-Based Monitors

Telnet Command	Description
perfAddReadMonitor	Count the number of SCSI Read commands
perfAddWriteMonitor	Count the number of SCSI Write commands
perfAddRWMonitor	Count the number of SCSI Read and Write commands
perfAddSCSIMonitor	Count the number of SCSI traffic frames
perfAddIPMonitor	Count the number of IP traffic frames

Example These commands add several filter-based monitors to port 2 and display the results.

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfAddReadMonitor 2
   SCSI Read filter monitor #0 added
sw1:admin> perfAddWriteMonitor 2
   SCSI Write monitor #1 added
sw1:admin> perfAddRWMonitor 2
   SCSI Read/Write monitor #2 added
sw1:admin> perfAddSCSIMonitor 2
   SCSI traffic frame monitor #3 added
sw1:admin> perfAddIPMonitor 2,
   IP traffic frame monitor #4 added
```

```
sw1:admin> perfShowFilterMonitor 2
   There are 5 filter based monitors defined on port 2.
```

KEY	ALIAS	OWNER_APP	OWNER_IP_ADDR	FRAME COUNT
0	SCSI Read	Telnet	N/A	0x0000000000000000
1	SCSI Write	Telnet	N/A	0x0000000000000000
2	SCSI R/W	Telnet	N/A	0x0000000000000000
3	SCSI Frame	Telnet	N/A	0x0000000000000000
4	IP Frame	Telnet	N/A	0x0000000000000000

Adding User-Defined Filter-Based Monitors

In addition to the standard filters (read, write, read/write, and frame count), you can create custom filters to qualify frames for statistics gathering to fit your own special needs.

To define a custom filter, use the `perfAddUserMonitor` Telnet command. You must specify a series of offsets, masks, and values. The following actions are performed. For all incoming frames, the switch:

- Locates the byte found in the frame at the specified `offset`
- Applies the mask to the byte found in the frame
- Compares the value with the given values in `perfAddUserMonitor`
- Increments the filter counter if a match is found

You can specify up to six different offsets for each port, and up to four values to compare against each offset.

If more than one offset is required to properly define a filter, the bytes found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment.

The value of the offset must be 0 or must be between 0 and 63, in decimal format. Byte 0 indicates the first byte of the Start of Frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus, only the SOF, frame header, and first 36 bytes of payload may be selected as part of a filter definition.

Offset 0 is a special case, which can be used to monitor the first four bytes of the frame (SOF). When the offset is **0**, the values are from 0 to 7, indicating the following:

0	SOFf
1	SOFc1
2	SOFil
3	SOFn1
4	SOFi2
5	SOFn2
6	SOFi3
7	SOFn3

The hardware can manage only a limited number of unique offsets and values. If the switch does not have enough resources to create a given filter, then other filters may have to be deleted to free up resources.

Example This command adds a filter-based monitor to count all FCP and IP frames received from domain 0x02 for port 2.

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfAddUserMonitor 2, 12, 0xff, 0x05, 0x08; 9, 0xff, 0x02 , FCP/IP
   User monitor #5 added
```

The FCP and IP protocols are selected by monitoring offset 12, mask 0xff and matching values of 0x05 or 0x08. Domain 2 is selected by monitoring offset 9, mask 0xff, and matching a value of 0x02.

The monitor counter is incremented for all incoming frames where byte 9 is 0x02 and byte 12 is 0x05 or 0x08.

Example The following command adds a special case filter-based monitor for SOFi3 on port 2:

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfAddUserMonitor 2, 0, 0xff, 6
User Monitor #6 added
```

Displaying Filter-Based Monitors

Use `perfShowFilterMonitor` to display all the filter-based monitors of a port. You can display a cumulative count of the traffic detected by the monitors, or you can display a snapshot of the traffic at specified intervals.

Intervals must be specified in multiples of five seconds, for example, 5, 10, 15, 20, 25, and so forth, because registers are scanned every five seconds.

This command displays all the filter-based monitors defined on the specified port. It displays all the valid monitor numbers and user-defined aliases on the specified port.

Example The following command displays filter monitor traffic on port 2 at an interval of once every six seconds. In the command output, `#CMDs` refers to the read, write, and read write counters, and `#Frames` refers to SCSI frame, IP frame, and user defined counters.

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfShowFilterMonitor 2, 6
```

0	1	2	3	4	5	6
#CMDs	#CMDs	#CMDs	#Frames	#Frames	#Frames	#CMDs
0	0	0	0	0	0	0
26k	187	681	682	682	494	187
26k	177	711	710	710	534	176
26k	184	734	734	734	550	184
26k	182	649	649	649	467	182
26k	188	754	755	755	567	184

Example The following command displays the cumulative frame count of all filter-based monitors defined on port 2. The KEY column lists the monitor numbers.

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfShowFilterMonitor 2
   There are 7 filter based monitors defined on port 2.

KEY   ALIAS        OWNER_APP    OWNER_IP_ADDR     FRAME_COUNT
0     SCSI Read    Telnet       N/A               0x0000000000002208
1     SCSI Write   Telnet       N/A               0x000000000000464a
2     SCSI R/W     Telnet       N/A               0x000000000000fd8c
3     SCSI Frame   WEB_TOOLS    192.168.169.40    0x00000000002c2229
4     IP Frame     WEB_TOOLS    192.168.169.40    0x0000000000000492
5     FCP/IP       WEB_TOOLS    192.168.169.40    0x0000000000000009
6     SCSI_RD      WEB_TOOLS    192.168.161.140   0x000000000000023a
```

Deleting Filter-Based Monitors

To delete a filter-based monitor, first list the valid monitor numbers using `perfShowFilterMonitor`, and then use `perfDelFilterMonitor` to delete a specific monitor. If you do not specify which monitor number to delete, you will be asked if you want to delete all entries.

If you do not specify a monitor number, then all filter monitors on the port are deleted.

Example The following commands display the monitors on port 4 (the monitor numbers are listed in the KEY column), and then delete monitor number 1 on port 4.

For the ED-12000B, a slot number and port number is needed.

```
sw1:admin> perfShowFilterMonitor 4
   There are 4 filter based monitors defined on port 4.
```

KEY	ALIAS	OWNER_APP	OWNER_IP_ADDR	FRAME_COUNT
0	SCSI Read	Telnet	N/A	0x0000000000002208
1	SCSI Write	Telnet	N/A	0x000000000000464a
2	SCSI R/W	Telnet	N/A	0x000000000000fd8c
3	SCSI Frame	WEB_TOOLS	192.168.169.40	0x00000000002c2229

```
sw1:admin> perfDelFilterMonitor 4, 1
   Monitor 1 is deleted
```

Clearing Filter-Based Monitor Counters

Before you clean statistics counters, verify all of the valid monitor numbers with user-defined aliases on a specific port using the `perfshowfiltermonitor` command, to make sure the correct monitor counters are cleared. To clear statistics counters for all or a specified filter-based monitor, use the `perfclearfiltermonitor` command. After the command has been executed, the telnet shell confirms that the counters on the monitor have been cleared.

In 4.1 and 3.1 issuing the command `portStatsClear` on a port will also result in all Filter-based monitors being cleared for all the ports in the same quad.

The example clears the statistics counters for a filter-based monitor 4 on port 2 in slot 1.

```
switch:admin> perfclearfiltermonitor 2, 4
Filter-based monitor number 4 counters are cleared
```

For the ED-12000B, a slot number and port number is needed.

Saving and Restoring Monitor Configuration

You can use `perfCfgSave` to save the current end-to-end and filter monitor configuration settings into flash memory. This enables the performance monitoring configuration to be saved over power cycles. You can use `perfCfgRestore` to restore the saved monitor configuration from flash memory, for example.

For example, if you power cycle the switch, and you want to use the same end-to-end and filter monitoring configuration that was in effect prior to the power cycle, do the following:

1. Use `perfCfgSave` to save the monitor configuration settings.
2. Power cycle the switch.

Use `perfCfgRestore` to restore the saved monitor configuration.

Example

```
sw1:admin> perfCfgSave
   This will overwrite previously saved Performance
   Monitoring
   settings in FLASH ROM.  Do you want to continue? [y|n]y
   Please wait ...
   Committing configuration...done.
   Performance monitoring configuration saved in FLASH
   ROM.

   sw1:admin> perfCfgRestore
   This will overwrite current Performance Monitoring
   settings in RAM.  Do you want to continue? [y|n]y
   Please wait ...
   Performance monitoring configuration restored from
   FLASH ROM.
```

Use `perfCfgClear` to clear the previously saved performance monitoring configuration settings from flash memory.

Example

```
sw1:admin> perfCfgClear
   This will clear Performance Monitoring settings in
   FLASH ROM.
   The RAM settings won't change.  Do you want to
   continue? [y|n]y
   Please wait ...
   Committing configuration...done.
   Performance Monitoring configuration cleared from
   FLASH.
```

A

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure A-1).

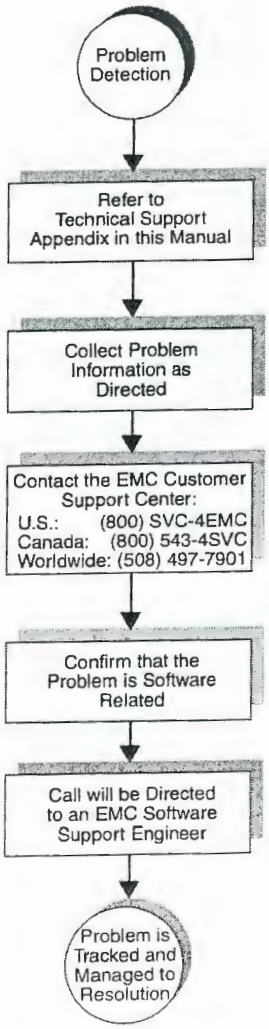


Figure A-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

```
http://powerlink.emc.com
```

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI.*

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP.*

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS.*

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex.*

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port.*

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode.*

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit.*

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL.*

M

Media See *Transceiver.*

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port.*

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

Index

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – MANUAL VOLUME 9

2003
PASTA 37

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

22.233 Paula

ANEXO SWITCH TIPO 03
PARTE 4/B

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

12 Firmware Download

This chapter contains the following sections:

Introduction

This chapter does not apply to EMC Connectrix B-Series switches at this time. To upgrade firmware on EMC Connectrix B-Series switches, please contact your EMC sales or service representative.

Perform a firmware download with Fabric Manager to concurrently download firmware to multiple switches and (optionally) reboot the switches simultaneously. Before you download firmware, verify that your task meets the following requirements:

- All switches that you choose to upgrade can run the firmware that you plan to download.
- All switches that you choose to simultaneously reboot reside on the same fabric.

Advantage

When you download firmware to multiple switches at once, then reboot the switches simultaneously, you use less time than if you update your switches individually.

Perform a Firmware Download to Multiple Switches

To download firmware to multiple switches, perform the following steps:

1. Log on to the switches that you want to upgrade. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. From the **Tools** menu, select **Firmware download to switches...** The **Firmware download to switches** window opens (Figure 12-1).

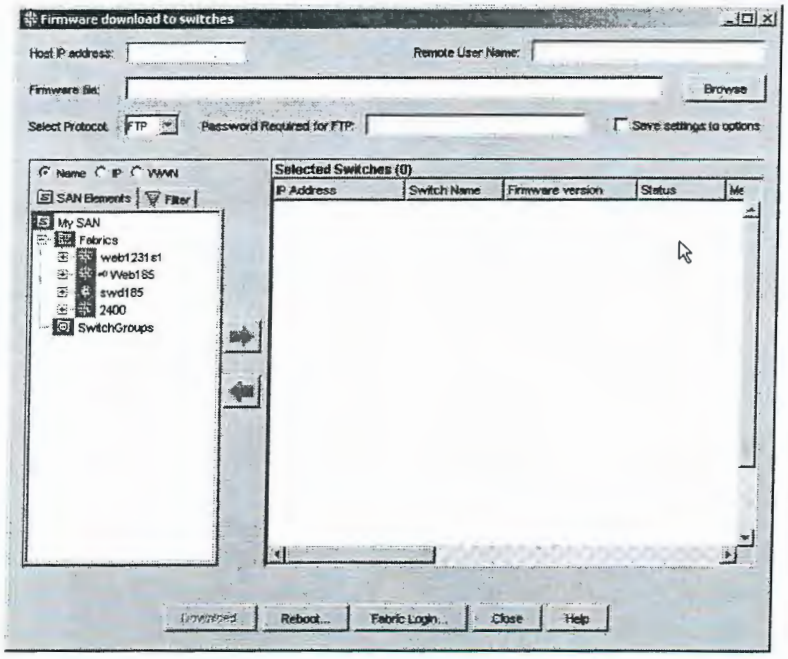


Figure 12-1 Firmware Download to Switches Window

3. In the **Host IP address** field, enter the IP address of the FTP server with the firmware file. If you have not configured file transfer options, select the **Save settings to options** checkbox to save your FTP settings as your file transfer options. For more information, refer to *Configure File Transfer Options* on page 4-16.

   You must click the **download** button to commit the file transfer options. If for any other reason you close this window, the file transfer options will not apply.

   ---

4. In the **Remote User Name** field, enter your user ID for the FTP server.
5. In the **Firmware file** field, enter the path and name of the firmware file (in UNIX format), or click **Browse** to navigate to the file.
6. From the **Select Protocol** pull-down menu, select **FTP**.

7. In the **Password Required for FTP** field, enter your password.
8. From the **SAN Elements** tab, select the switches that you want to upgrade and move them to the **Selected Switches** window. You can:
   - Navigate to a switch, click the switch, and then click the right arrow.
   - Click and drag a switch from the **SAN Elements** tab to the **Selected Switches** window.
   - Press and hold CTRL, click multiple switches, and click the right arrow.
   - Press and hold CTRL, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the **Selected Switches** window.
   - Click and drag a fabric to the **Selected Switches** window to move add all of the switches in that fabric to the **Selected Switches** window.

   If you want to download firmware to a dual-switch chassis, *you can only download firmware to one logical switch at a time.* Furthermore, you only need to download the firmware to one logical switch in a dual-switch chassis. If you add both of the logical switches in a chassis to the **Selected Switches** window, you will receive an error prompt when you click **Download**.

   ---

9. Click **Download**. When the download completes, click **Reboot...** to open the **Sequenced Reboot** window.

   If the switch loses network connectivity during the firmware download from Fabric Manager, the firmware download action will time out after 25 minutes for switches running firmware v2.x/3.x and after 80 minutes for switches running firmware v4.x.

   No error message is returned when the firmware download process gets interrupted.

Control Firmware Download Reboots

Switches do not automatically reboot after you perform a firmware download. Fabric Manager gives you the opportunity to create a download sequence so you can control the order in which the switches reboot. For more information, refer to *Perform a Sequenced Reboot* on page 18-5.

13 ISL Checking

This chapter contains the following sections:

Introduction

Enable interswitch link checking (ISL) to monitor any changes to your ISL topology. When you enable ISL Checking, Fabric Manager takes a snapshot, or *stamp*, of your ISLs. Whenever you add, remove, or change an ISL, Fabric Manager compares the change to the stamp and triggers an event when mismatches occur. Events change the color and status of related icons in the Fabric Manager display and create log entries. ISL Checking monitors when you do the following:

- Add a new ISL to the fabric
- Remove an ISL from the fabric
- Remove all ISLs between two switches in a fabric
- Plug an existing ISL into a different port on the same switch

Assign Color Status Settings

Before you enable ISL Checking, configure ISL Checking options to assign an alarm status level to each ISL Checking event. For more information on the individual ISL Checking options, refer to *ISL Status Options* on page A-12.

When an event occurs, the appropriate element changes to the color that you assign. To assign color status, perform the following steps:

1. From the **File** menu, select **Options...** The **Options** window opens.
2. Click the **ISL Status** branch in the **Configurations** navigation tree. ISL Status options appear in the window (Figure 13-1).

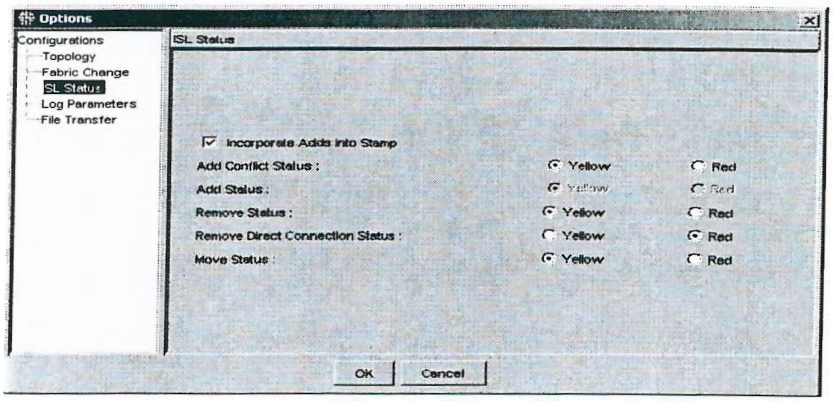


Figure 13-1 ISL Status Options

3. Click the radio buttons that assign the colors that you choose; then click **OK**.

Enable/Disable ISL Checking

To enable or disable ISL Checking, perform the following steps:

1. Assign color status settings. For more information, refer to *Assign Color Status Settings* on page 13-3.
2. In the **SAN Elements** tab, click the fabric that you want to check or no longer want to check.
3. From the **Actions** menu, select **ISL > ISL Checking**. A checkmark appears next to **ISL Checking** to indicate that you have enabled it. The checkmark will disappear when you disable it.

When you enable ISL Checking on a fabric, a gold center appears on the icon of the fabric in the **SAN Elements** tab. When you disable ISL Checking, the gold center disappears.

Stamp/Restamp

When you activate ISL Checking, Fabric Manager takes a stamp of your topology so it can compare changes and register events. If you make permanent changes that do not match the stamp, you must restamp the fabric so that Fabric Manager knows to match your topology against the correct baseline. To restamp your fabric, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to restamp.
2. From the **Actions** menu, select **ISL > Restamp**.

Stamps take snapshots of domain IDs, so if you change the domain ID of a switch, a remove event occurs and you must restamp the fabric.

Incorporate Adds into a Stamp

ISL Checking gives you the opportunity to automatically incorporate new ISLs into the stamp (including if you add new ISLs to switches that did not connect to the fabric before). To incorporate new ISLs and switches into your stamp when you add them to your fabrics, perform the following steps:

1. From the **File** menu, select **Options...** The **Options** window opens.

2. Click the **ISL Status** branch in the **Configurations** navigation tree. ISL Status options appear in the window.
3. Click the **Incorporate Adds into Stamp** checkbox and click **OK**.

Monitor ISL Changes

When your fabric experiences a change that triggers an ISL Checking event, Fabric Manager changes the color (as per your configuration) of appropriate icons to alert you. You can investigate the status change with Event view and Topology view.

ISL Changes and Event View

The **Current Status Reason** window displays each switch that changed from HEALTHY/OK status to any other status level. The window includes the new status of each switch and the reason that the status changed. The **Event Log** window appears on the bottom half of the display and includes events that preceded the status change. Figure 13-2 reflects ISL Checking color changes in Event view.

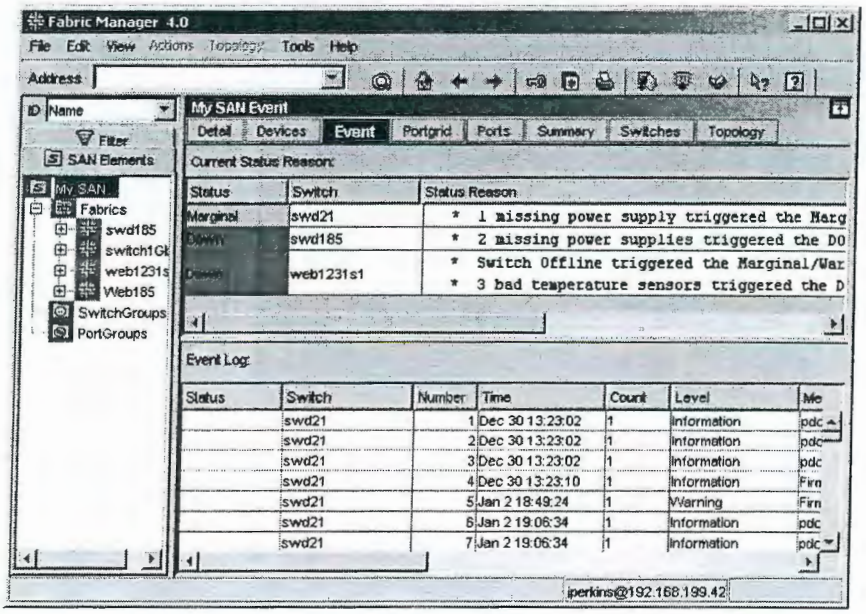


Figure 13-2 ISL Checking Status in Event View

ISL Changes and Topology View

When you enable Fabric Checking, the nodes, links, and link bundles in Topology view change color to reflect your ISL Checking color status settings.

When a direct-connect remove event occurs, Topology view does not change color to reflect an ISL event.

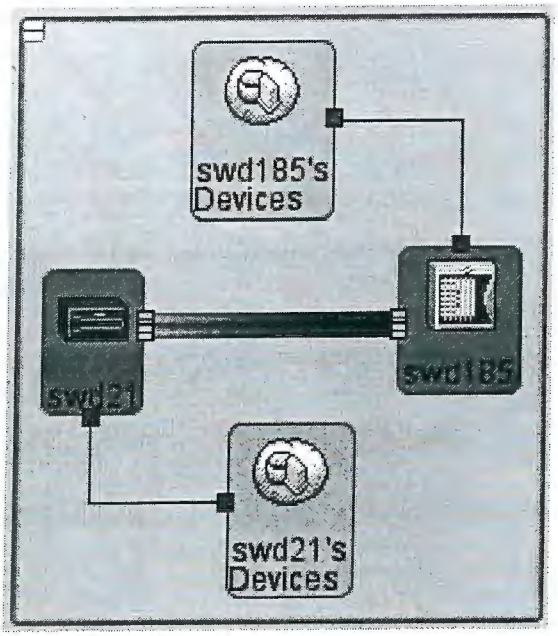


Figure 13-3 ISL Checking Status in Topology View

14 Fabric Checking

This chapter includes the following sections:

Introduction

You can configure the Fabric Checking feature to monitor the fabric and register events when you add switches to, or remove switches from, the fabric. When you add or remove a switch from a selected fabric, Fabric Checking adds an entry to the switch event log and changes the status color of the fabric. You can configure Fabric Checking to ignore additions to the fabric, but the software always registers an event when you remove a switch.

Fabric Manager polls the fabric every fifteen seconds to determine if the fabric has changed. Table 14-1 lists the changes that Fabric Checking monitors and describes how the software responds to the change.

Table 14-1 Fabric Checking Alerts

Change	Response
Switch disconnects from fabric	Fabric Manager creates a *ghost* switch image that lasts until you restore the switch to the fabric or disable Fabric Checking. The following actions take place to represent the changes in Fabric Manager: ◆ Fabric Manager adds an entry to the switch event log stating that the switch has been removed from the fabric. ◆ Fabric Manager changes the status color of the fabric. ◆ A ghost switch image appears in the Topology View, At-a-Glance view(s), and the Switch table. ◆ Entries for the ghost switch are removed from the portgrid, ports, and devices tables.
Switch connects to fabric	Fabric Manager adds an entry to the switch event log and changes the status color of the fabric.

Fabric Checking monitors *switches* (not devices) removed from and added to a fabric.

Advantage

Fabric Checking allows users to know when changes occur in the fabric. If you administer a fabric that you want no one to add switches to or remove switches from, Fabric Checking helps you monitor that activity.

Enable Fabric Checking on a Fabric

To enable Fabric Checking, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to check.
2. From the **Actions** menu, select **Fabric Checking**. A dark blue ring appears around the icon in the **SAN Elements** tab, the Topology view, and the At-a-Glance views to indicate that you enabled Fabric Checking.

Reset Fabric Checking

Reset Fabric Checking after you make a permanent addition or deletion to your fabric. To reset Fabric Checking, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you want to reset.
2. From the **Actions** menu, select **Fabric Checking** to disable fabric checking on the fabric.
3. From the **Actions** menu, select **Fabric Checking** to enable Fabric Checking with the new topology.

Automatically Enable Fabric Checking on All Fabrics

To automatically enable fabric checking on all fabrics that Fabric Manager discovers, perform the following steps:

1. From the **File** menu, select **Options...** The **Options** dialog box appears (Figure 14-1).

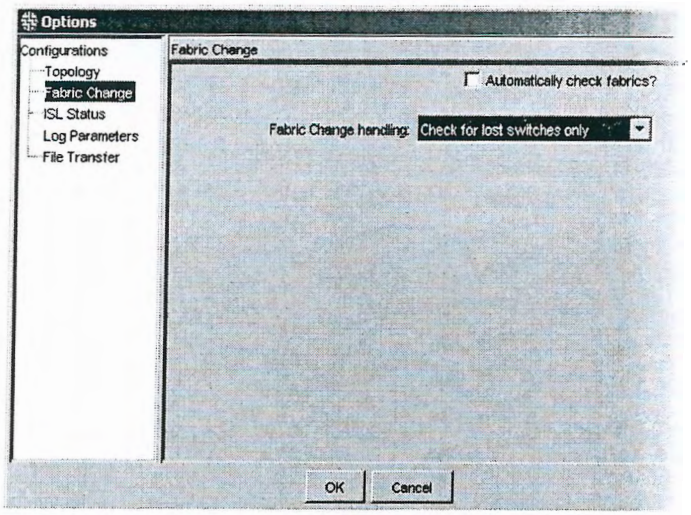


Figure 14-1 Options Window for Fabric Checking

2. In the **Configurations** tree, click **Fabric Change**. The **Fabric Change** dialog box appears in the right-hand window.
3. In the **Fabric Change** dialog box, select the **Automatically check fabrics?** checkbox and click **OK**.

Disable Fabric Checking

To disable Fabric Checking, perform the following steps:

1. In the **SAN Elements** tab, click the fabric that you no longer want to check.
2. From the **Actions** menu, select **Fabric Checking**. The check mark beside **Fabric Checking** is removed.

Monitor Fabric Checking in Topology View

When you remove a switch from a checked fabric, the switch appears *ghosted* in Topology view and the links to the switch no longer appear. When you return the switch, the standard node replaces the *ghost* node.

Figure 14-2 displays a fabric that runs Fabric Checking.

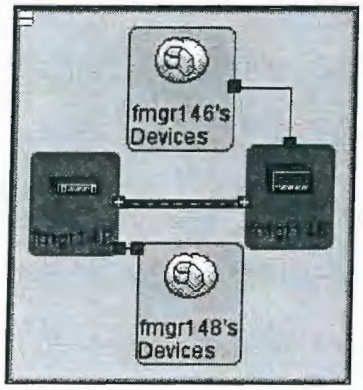


Figure 14-2 Fabric Before a Remove Event

Figure 14-3 displays the same fabric after the administrator removes a switch. Switch fmgr146 appears ghosted.

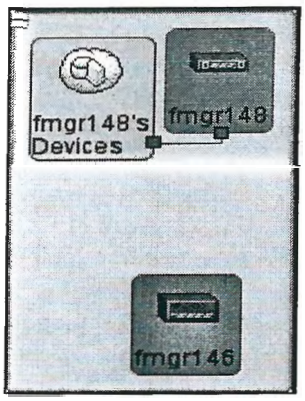


Figure 14-3 **Fabric After a Remove Event**

If ISL Checking and Fabric Checking are both enabled, and a switch is removed from the fabric, a red color link will be displayed in the Topology view connecting the ghosted switch node to the original switch to which it was connected.

---

15 Fabric Merge Check

This chapter includes the following sections:

Introduction

Perform a fabric merge check to determine if two fabrics will segment if you merge them. Fabric Manager provides the fabric merge check to compare various configuration elements of two fabrics before you connect those fabrics. Fabric Manager extracts copies of configuration elements from each fabric that can cause the fabric to segment and compares them in memory for inconsistency. Inconsistencies are displayed in the merge-check results window. Fabric Manager performs the following tests during a fabric merge check:

- Domain ID test
- TimeOutValue test
- Buffer-to-Buffer Credit test
- Disable Device Probe test
- Route Priority per Frame test
- Sequence Level Switching test
- Suppress Class F test
- Long Distance Mode test
- InterOp Mode test
- Data Field Size test
- VC Encoding test
- PID test
- Zoning test (only runs on non-secure fabrics)
- VC Priority test

The following tests only run in a secure fabric:

- Security test
- FCS Policies test
- Version Stamp test
- Management Server Platform test

Check Fabrics

You can check any two fabrics that you have discovered. To perform a fabric merge check, perform the following steps:

1. Log on to the switches that you want to check. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. From the **Tools** menu, select **Fabric Merge...** The **Fabric Merge Check** dialog box opens.
3. From each **fabric** pull-down menu, select one of the two fabrics that you want to merge and click **Check...** A **Merge Check Results** list appears and identifies the inconsistencies between the fabrics.

If you run a Fabric Merge Check between a secure fabric and a nonsecure fabric, the results of the Security, FCS Policies, Version Stamp, and Management Server Platform tests will display the following message:
`Not applicable to subject fabrics.`

Best Practices

If you plan to add a switch to a fabric that uses zoning, discover that switch with Fabric Manager and run a merge check between that switch and the fabric to which you plan to add it. This check will identify any zoning and configuration mismatches before you physically connect the switch.

16 Comparing Configurations

This chapter contains the following sections:

Introduction

Fabric Manager can compare the configuration files of your switches to a *baseline* configuration to:

- Validate and ensure consistent configuration settings among the switches in your fabric.
- Propagate configuration settings to switches in your fabric.
- Store a selection of configuration settings that you can easily propagate throughout your fabric.
- Troubleshoot a switch.

Table 16-1 explains the two sources that Fabric Manager can use as baselines.

Table 16-1 Baseline Sources

Source	Explanation
Switch	You can compare multiple switches to one switch that you identify as a baseline.
File	You can save the configuration file of a switch as a file on a FTP server, and then compare switches to that file or propagate that file to switches.

You can save portions of a configuration to a file so you can propagate fabric-wide settings but leave switch-specific settings untouched. For instance, you can save Fabric Watch configuration settings to a baseline, then propagate those settings to an entire fabric and not alter the name of any switch in the fabric.

Best Practices

The following best practices describe tasks you can perform with the **Save Baseline...** tool to administer your fabric more efficiently.

- Propagate a baseline configuration to each new switch that you add to a fabric to ensure that the switch is compatible with the fabric.
- Propagate the baseline of one fabric throughout a second fabric before you merge the fabrics.
- Propagate a baseline configuration throughout a fabric to ensure consistent Fabric Watch and SNMP settings.

- Create and store multiple baselines that serve different purposes so you can quickly adapt your fabric when it switches function.

  You can create a limitless number of baselines.

- Use baselines to recover fabric and switch settings.

Save a Baseline Configuration to a File

If you just discovered a fabric and want to save a baseline, wait about 60 seconds to let Fabric Manager discover all port, device, and ISL information. If you do not wait, you will receive incomplete results when you run the baseline compare.

Save a baseline from a single switch in a fabric. You can export the following categories of information from the configuration file to the baseline:

- Settings that you can normally assign with the `configure` command
- Settings for Fabric Watch and SNMP

When you create your baseline, Fabric Manager gives you the opportunity to choose what settings you want to add to the baseline and what settings you want to omit from the baseline. To save a baseline, perform the following steps:

1. Configure file transfer settings if you have not already done so. For more information, refer to *Configure File Transfer Options* on page 4-16.
2. Log in to the switch with the configuration that you want to save as a baseline. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
3. From the **Tools** menu, select **Config** > **Save Baseline...** The **Save Baseline -- Configuration Template Selection** dialog box opens.
4. Select **Full Configuration** and click **Next**. The **Save Baseline -- Switch Selection** window opens.
5. From the **SAN Elements** tab, choose the switch with the configuration that you want to save, and then click the right arrow to add it to the right-hand window.

6. Click **OK**. The **Save Baseline -- Parameter Selection** window opens.
7. Select the checkboxes for each setting or group of settings of the configuration file that you want to save to the baseline. Expand and collapse the navigation tree to drill down into your options.
8. Click **Save**. The **Save base file** dialog box opens.
9. Enter a name for your baseline, choose a folder to store it, and click **Save**.

Compare Switches to a Baseline

When you compare the configuration of a switch to a baseline, Fabric Manager identifies and lists all parameters that do not match. Compare the configuration of one or more switches to a baseline when:

- You plan to merge two fabrics.
- You plan to add a new switch to a fabric.
- You want to verify that Fabric Watch and SNMP settings are consistent across a fabric.
- A fabric segments and you need to troubleshoot the problem.

If you just discovered a fabric and want to run Fabric Backup or Diff with Backup, you need to wait about 60 seconds to let Fabric Manager discover all port, device, and ISL information. If you don't wait, you will have incomplete results when running the Fabric Backup or Diff with Backup.

Compare Switches to a Baseline File

To compare switches to a baseline file, perform the following steps:

1. From the **Tools** menu, select **Config > Compare/Download from File**. The **Compare/Download from File -- Select Baseline Configuration** dialog box opens.
2. Navigate to the baseline file and click **Open**. The **Compare/Download from File -- Target Switch Selection** window opens.
3. From the **SAN Elements** tab, select the switches that you want to compare and move them to the right-hand window. You can:

- Navigate to a switch, click the switch, and then click the right arrow.
- Click and drag a switch from the **SAN Elements** tab to the right-hand window.
- Press and hold CTRL, click multiple switches in the **SAN Elements** tab, and click the right arrow.
- Press and hold CTRL, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the right-hand window.
- Click and drag a fabric to the right-hand window to move add all of the switches in that fabric to the window.

4. Click **OK**. The **Compare/Download from File -- Switch Configuration comparison and Download** window appears and compares the configuration(s) of the switch(es) to the baseline.

To apply this baseline to the switches that you selected, click **Apply Baseline...**

Compare Switches to a Baseline Switch

To compare switches to a baseline switch, perform the following steps:

1. From the **Tools** menu, select **Config > Compare/Download from Switch**. The **Compare/Download from Switch -- Source Configuration Selection** window opens.
2. Navigate to the switch that you want to use as a baseline and click the right arrow to move that switch to the right-hand window.
3. Click **OK**. The **Compare/Download from Switch -- Target Switch Selection** window opens.
4. From the **SAN Elements** tab, select switches you want to compare and move them to the right-hand window. You can:
   - Navigate to a switch, click the switch, and then click the right arrow.
   - Click and drag a switch from the **SAN Elements** tab to the right-hand window.
   - Press and hold CTRL, click multiple switches in the **SAN Elements** tab, and click the right arrow.

- Press and hold CTRL, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the right-hand window.
- Click and drag a fabric to the right-hand window to move add all of the switches in that fabric to the window.

5. Click **OK**. The **Compare/Download from Switch -- Switch Configuration comparison and Download** window appears and compares the configuration(s) of the switch(es) to the baseline.

To apply this baseline to the switches that you selected, click **Apply Baseline...**

Customize Baseline Templates

When you save a baseline configuration, Fabric Manager requires that you choose a configuration template. The templates appear in the **Save Baseline -- Configuration Template Selection** dialog box (Figure 16-1).

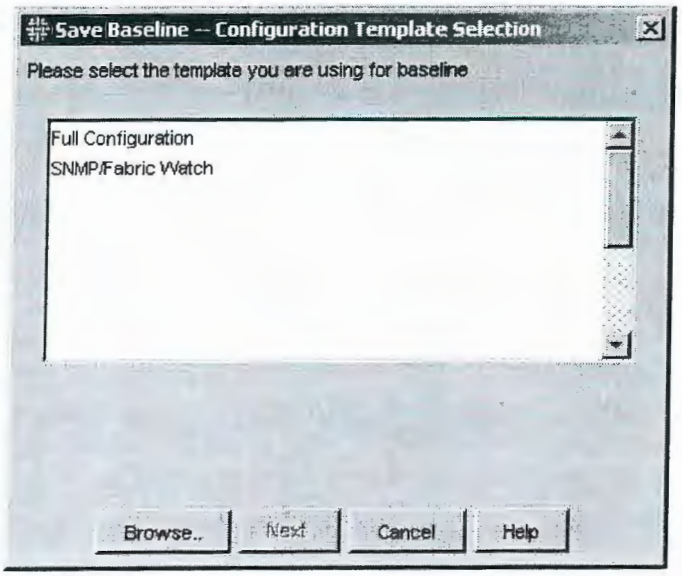


Figure 16-1 Save Baseline—Configuration Template Selection Dialog Box

The template that you choose determines what parameters appear in the **Save Baseline -- Parameter Selection** dialog box (Figure 16-2.)

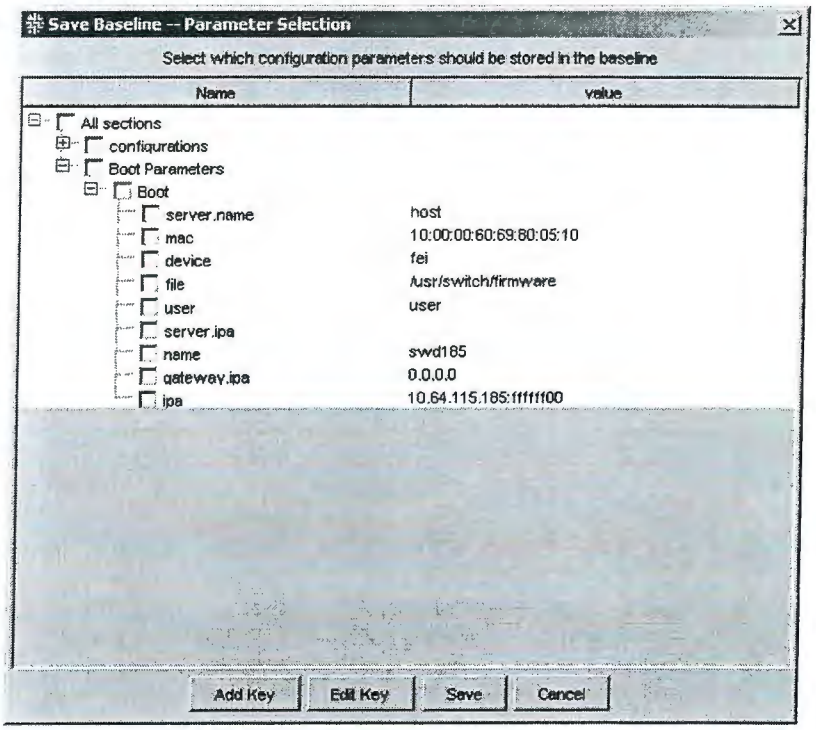


Figure 16-2 Save Baseline -- Parameter Selection Dialog Box

Fabric Manager provides two templates, but you can create custom templates or edit the existing templates. To create a custom template, create an XML file (as defined next) and save it in the **Fabric Manager > baseline > template** directory on your Fabric Manager server. The **Full Configuration** and **SNMP/Fabric Watch** template files appear in this directory.

Anatomy of Template Files

To customize a baseline template file, you must define custom XML tags. This section describes those tags.

Description Tag

The **Description** tag encloses the summary tag, which defines what template title appears in the **Save Baseline -- Configuration Template Selection** dialog box. The example that follows displays **My Template** in the dialog box.

Example

```
<Description>
   <summary>My Template</summary>
   <detail>This will show my custom parameters</detail>
</Description>
```

The results of this configuration appear in Figure 16-3.

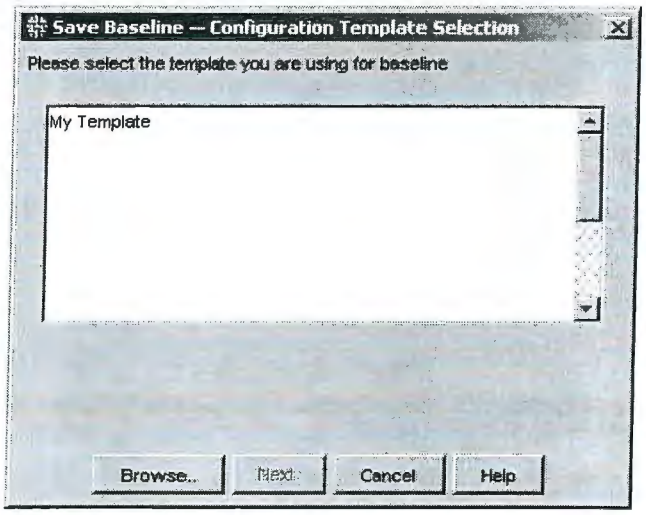


Figure 16-3 Description Change Results

section Tag

Each **section** tag adds a section from the configuration file to the template. Sections appear in the configuration file as text in square brackets ([,]). Section tags contain prefix tags.

In the example that follows, the **section** tag uses a Boot Parameters **value** attribute to add the [Boot Parameters] section of the configuration file to the display. It uses a Boot Parameter **text** attribute to identify the checkbox in the **Save Baseline -- Parameter Selection** dialog box. This **section** tag includes a **prefix** tag to add parameters to the section.

Example

```
<section value="Boot Parameters" text="boot parameters">
   <prefix ID="boot" text="Boot"/>
</section>
```

The results of this configuration appear in Figure 16-4.

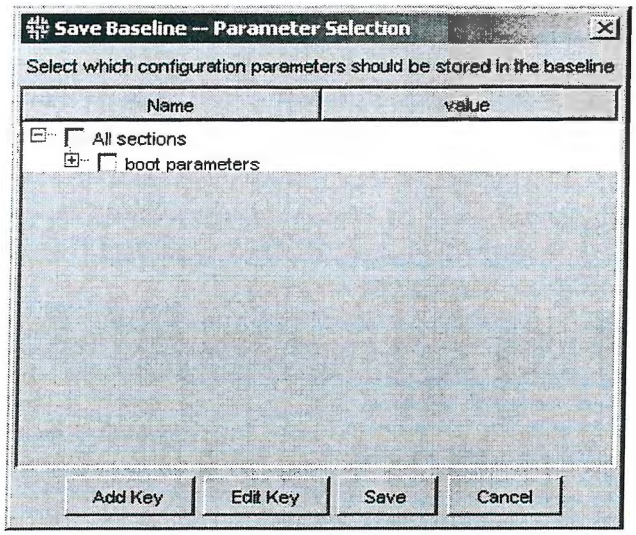


Figure 16-4 Section Change Results

prefix Tag

The **prefix** tag adds parameters to the template. Every parameter in the configuration file includes a prefix before the first dot (.). Set the **ID** attribute of the prefix tag to add all configuration file parameters that use that prefix to the template. For instance, if you set the ID attribute to **route**, parameters such as route.delayReroute, route.embeddedPortBcast, and route.stickyRoutes appear in your template. Set the **text** attribute to define the text that accompanies the parameter in the **Save Baseline -- Parameter Selection** dialog box.

The example that follows adds all parameters in the configuration file that begin with **boot.** to the template.

Example

```
<prefix ID="boot" text="Boot"/>
```

The results of this configuration appear in Figure 16-5.

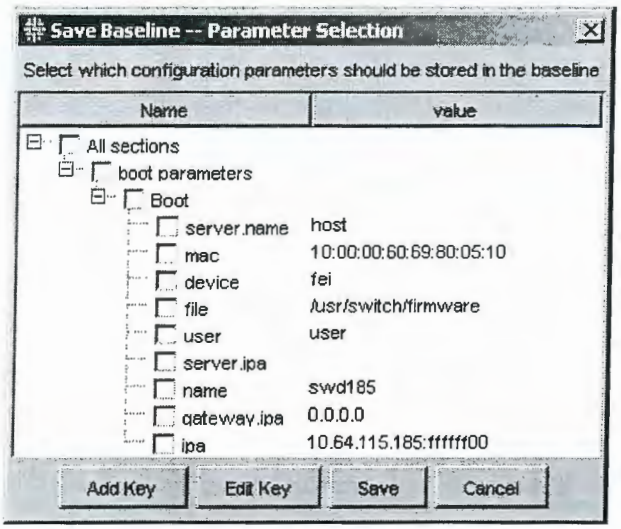


Figure 16-5 **Prefix Change Results**

Create or Edit a Template

To create a custom baseline template, perform the following steps:

1. Open `fullBaseLineTemplate.xml` in a text editor.

   In a Windows environment, Notepad *will not work*. To edit the XML document, you must open the file in WordPad or a similar application that recognizes carriage returns.

2. Edit the text that appears between the **<summary>** and **</summary>** tags to configure the template name that appears in the **Save Baseline -- Configuration Template Selection** dialog box.
3. Add or remove **section** tags to include or remove sections from the **Save Baseline -- Parameter Selection** dialog box.
4. Add or remove **prefix** tags to **section** tags to include or remove parameters from the **Save Baseline -- Parameter Selection** dialog box.

   In each section, only include prefixes that appear in the analogous section in the configuration file.

5. Save the file to customize the existing file, or save the file in the same directory with a different filename to create a new configuration.

17 Complete Fabric Backup and Compare

This chapter contains the following sections:

Introduction

The Backup action in Fabric Manager aggregates a number of the features of the application to create a thorough backup file of your entire fabric. This action backs up the following information about a fabric to one file:

- The configuration file of every switch in the fabric
- The license keys for every switch in the fabric
- A list of switches that belong to the fabric
- An ISL stamp

The Backup action does not store the current ISL stamp. It creates a stamp of the ISLs as they appear *at the moment of the backup.*

- All zone definitions (and notes the active zone)
- Which firmware version each switch runs
- Name server information

Once you back up your fabric, you can compare the settings of your live fabric to the settings in your baseline file. Fabric Manager displays the discrepancies between the two in HTTP format.

Back Up a Fabric

Verify that Fabric Manager has discovered all fabric information before you perform a backup. If you just discovered a fabric and want to run a backup, wait about 60 seconds to let Fabric Manager discover all port, device, and ISL information. If you do not wait, you will receive incomplete results when you run the backup compare.

To back up a fabric, perform the following steps:

1. From the **SAN Elements** tab, click the fabric that you want to back up.
2. From the **Actions** menu, select **Backup...** The **Backup fabric configuration-Select a folder** dialog box opens.
3. Select a directory to store your backup file and click **Backup now**. A Backup result details window opens and displays the contents of your new backup file.

Compare a Fabric to a Backup

1. From the **SAN Elements** tab, click the fabric that you want to check against a backup.
2. From the **Actions** menu, select **Diff with backup...** The **Diff fabric configuration with backup** dialog box opens.
3. Navigate to the directory that contains your backup and click **Diff**. The **Live/Backup Configuration Difference** window opens and lists the discrepancies between your live fabric and your backup.

18 Sequenced Reboot

This chapter contains the following sections:

Introduction

With Fabric Manager, you can define groups of switches that reboot simultaneously, then configure groups to reboot sequentially. Reboot groups let you simultaneously reboot switches that run the same firmware, serve the same function, reside in the same physical location, or share any other attribute by which you want to group them. Table 18-1 defines the critical terms in this section.

Table 18-1 Sequenced Reboot Terms

Term	Definition
Reboot group	A group of switches (from the same fabric) that reboot simultaneously.
Time-out	Occurrence where a fabric does not stabilize within the amount of time that you configure.
Stabilization	Occurrence where all WWNs of a fabric appear in the `fabricshow` command output.

Reboot groups consist of one or more switches from a single fabric. You cannot group switches from different fabrics. Any given switch can only belong to one reboot group.

Advantage

Sequenced reboots give sections of your SAN an opportunity to reboot and stabilize before other switches in the fabric begin to reboot, which reduces the load of inter-switch traffic on the SAN.

Reboot Strategies

Use the following reboot strategies to take full advantage of this feature:

- Simultaneously reboot switches that run the same firmware
- Simultaneously reboot switches of the same model
- Reboot the core switches of a fabric, and then the edge switches
- Reboot the backbone of a large SAN, and then reboot other sections
- Reboot distant physical locations sequentially

Create a Reboot Group

To create a reboot group, perform the following steps:

1. From the **Tools** menu, select **Reboot** > **Create Reboot Sequence...** The **Create or change reboot groups and sequence** window opens.
2. Select a fabric from the **Select Fabric** pull-down menu.
3. Click **Create...** The **Create reboot group** dialog box opens.
4. In the **Name of the Reboot Group** field, type a name for the group.
5. In the **Fabric Stabilization timeout** field, specify the amount of time for the fabric to stabilize.
6. In the **What to do if timeout occurs?** field, click one of the following radio buttons:
   - **Prompt** displays a prompt when a timeout occurs that asks you if you want to continue.
   - **Continue** continues the reboot sequence when a time-out occurs.
   - **Abort** terminates the reboot sequence when a time-out occurs.
7. In the **Delay After Fabric Stabilization** field, configure the amount of time that must elapse before the next reboot in the sequence begins.

   Fabric Manager considers a fabric stable when all WWNs appear in the `fabricshow` command output.

   ---

8. Click **OK**. Your reboot group appears in the **Reboot Groups** tree.

When your reboot group appears in the **Reboot Groups** tree, bracketed text appears next to the name of the group. The text in the brackets represents the fabric stabilization time-out duration, time-out option, and delay after fabric stabilization options that you configured.

Example `[1m,P,2m]`

In this example, `1m` identifies a stabilization time-out of one minute, `P` identifies that Fabric Manager will prompt you if a time-out occurs, and `2m` indicates that two minutes will elapse before the next reboot in the sequence begins.

Assign Switches to a Reboot Group

To assign switches to a reboot group, perform the following steps:

1. From the **Tools** menu, select **Reboot** > **Create Reboot Sequence...** The **Create or change reboot groups and sequence** window opens.
2. Select a fabric from the **Select Fabric** pull-down menu. The switches in that fabric appear in the **Unassigned Switches** window.
3. Click the reboot group that you want to populate.
4. Click a switch that you want to add to the group, and then click the left arrow; then click **OK**.

To add multiple switches at once, press and hold CTRL and click each switch that you want to add; then click the left arrow.

Single Switch Groups

Create a single switch group to account for individual switches that you have not assigned to a group. Single switch groups include these individual switches in the reboot sequence.

To create a single switch group, perform the following steps:

1. From the **Tools** menu, select **Reboot** > **Create Reboot Sequence...** The **Create or change reboot groups and sequence** window appears.
2. Select a fabric from the **Select Fabric** pull-down menu.
3. Select a switch from the **Unassigned Switches** window. To create multiple single-switch groups, select multiple switches. Each switch will be made into its own group.
4. Click the **Create single switch groups...** button. The **Create single switch reboot groups** dialog box appears.
5. In the **Name of the Reboot Group** field, type a name for the group(s).
6. In the **What to do if time-out occurs?** field, click one of the following radio buttons:
   - **Prompt** displays a prompt when a time-out occurs that asks you if you want to continue.
   - **Continue** continues the reboot sequence when a time-out occurs.
   - **Abort** terminates the reboot sequence when a time-out occurs.

7. In the **Delay After Fabric Stabilization** field, configure the amount of time that must elapse before the next reboot in the sequence.

   Fabric Manager considers a fabric stable when all WWNs appear in the `fabricshow` command output.

8. Click **OK**. Your reboot group appears in the **Reboot Groups** tree.

Perform a Sequenced Reboot

To set up a sequenced reboot, perform the following steps:

1. Log in to the switches that you want to reboot. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. From the **Tools** menu, select **Reboot** > **Sequenced Reboot...** The **Sequenced Reboot** window appears.
3. Select a fabric from the **Select Fabric** pull-down menu.
4. In the **Reboot Groups** tab, click the group that you want to reboot first, and then click the right arrow to add it to the **Selected Switches** window.
5. Repeat step 4 to add additional groups in the order that you want them to reboot.

   To rearrange the order of the reboot sequence, click the up and down arrow keys in the **Sequenced Reboot** window.

6. Click **Fastboot** or **Reboot** to begin the sequenced reboot. Fabric Manager will prompt you several times to be sure that you want to proceed. The prompt will present potential problems in your fabric. A message appears at the end of the reboot sequence to list successful and unsuccessful reboots.

19 Emulex HBA Firmware Download

This chapter contains the following sections:

Introduction

Fabric Manager supports up to 50 firmware downloads to multiple HBAs simultaneously.

You can only perform a firmware download to an HBA if the HBA is connected to a switch running firmware versions 3.1.0 or 4.1.0.

Download Firmware to an HBA

To download firmware to one or more HBAs, perform the following steps:

1. Log on to a switch (or switches) with version 3.1.0 or 4.1.0 firmware loaded and has FDMI-capable HBAs connected to it (or them). For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. From the **Tools** menu, select **Firmware download to HBAs...** The **Firmware download to HBAs** window opens (Figure 19-1).

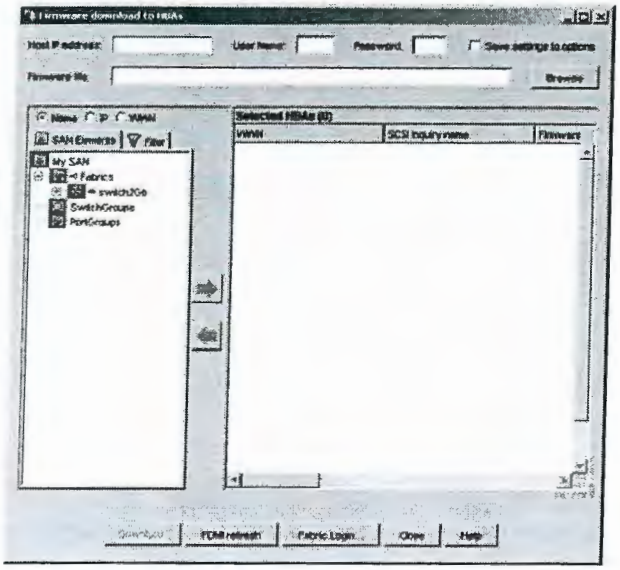


Figure 19-1 Firmware Download to HBAs Window

3. In the **Host IP address** field, enter the IP address of the FTP server with the firmware file. The IP address appears automatically if you have already configured file transfer options. For more information, refer to *Configure File Transfer Options* on page 4-16. If you have not configured file transfer options, select the **Save settings to options** checkbox to save your FTP settings as your file transfer options.
4. In the **User Name** field, enter your user ID for the FTP server.
5. In the **Firmware file** field, enter the path and name of the firmware file (in UNIX format), or click **Browse** to navigate to the file.
6. In the **Password** field, enter your password.
7. From the **SAN Elements** tab, select HBAs you want to upgrade and move them to the **Selected HBAs** window. You can:
   - Navigate to an HBA, click the HBA, and then click the right arrow.
   - Click and drag a HBA from the **SAN Elements** tab to the **Selected HBAs** window.
   - Press and hold CTRL, click multiple HBAs, and click the right arrow.
   - Press and hold CTRL, click multiple HBAs, and click and drag the HBAs from the **SAN Elements** tab to the **Selected HBAs** window.
   - Click and drag a fabric to the **Selected HBAs** window to add all of the HBAs in that fabric to the **Selected HBAs** window.

Non-FDMI-capable HBAs will appear with a grey background. In addition, if Fabric Manager detects that the device is no longer in the Name Server, the device will be displayed with a grey background in the **Firmware Download to HBAs** window until the device logs in to the Name Server again.

8. Click the **Download** button to begin the firmware download. Fabric Manager will prompt you with a confirmation dialog box.
9. Click **OK** to proceed or **Cancel** to abort. Fabric Manager will provide a report of successful and unsuccessful downloads.

Click **Refresh FDMI** to refresh FDMI information available in the **Firmware Download to HBA** window for the selected HBAs.

20 Troubleshooting

This chapter contains the following sections:

Introduction

This chapter provides solutions to problems that you may encounter as you manage your SAN with Fabric Manager. If you cannot troubleshoot the problem successfully, please contact customer support.

View Fabric Manager Application Log

When you contact customer support, they may ask you for information from the Fabric Manager Application log. This log is different from the Event view. The Fabric Manager Application Log logs events for the application, not necessarily the SAN or its elements.

To view events in the Fabric Manager Application log, click the **File** menu and select **Log...** After you open the window, you can filter what information appears in the window.

Filter Events

To filter events, perform the following steps:

1. From the **File** menu, select **Log...** The **Fabric Log** dialog box opens.
2. Click **Filter**. The **Filter** dialog box opens.
3. Enter the criteria for the messages that you want to filter, and then click **Filter**. The messages that fit your criteria appear in the log.

Problems and Solutions

The sections in this chapter describe problems that you may experience with Fabric Manager. A solution to the problem follows each section.

Fabric Manager Client Cannot Access the Server

Verify that the client uses the same port as the server. For more information, refer Figure 2-7 on page 2-7.

Switches and Hosts No Longer See an HBA After a Firmware Download to the HBA

During the firmware download to HBA process, if the switch or the host (that the HBA is attached to) is rebooted, the firmware in the HBA flash memory can become corrupted and the HBA will not be able to log in to the switch or respond to the query from the switch. Thus, from both the Fabric Manager and the switch point of view, this HBA does not appear and drops out of the Name Server list. To solve this problem, use HBAnyware on the attached host and reload the firmware on the HBA.

503 Service Unavailable/ Overloaded Error Appears

Poll the switch with fewer Fabric Manager clients.

This error indicates that Fabric Manager discovered a switch whose Web server is generating the 503 error. When a switch generates this error after Fabric Manager has already discovered the switch, the error only appears in the error log. Although switches can appear as unreachable in FM when they experience this error, this error occurs more frequently on switches that run firmware versions 2.x and 3.x.

A Zero-Switch (Empty) Fabric Appears in the SAN Elements Tab

When a switch segments from a fabric that runs Fabric Checking and then rejoins the fabric, an empty fabric remains in the **SAN Elements** tab. To remove this empty fabric, select it, and then disable Fabric Checking on that fabric. It will disappear from the tab.

A

File Menu Reference

This appendix has the following sections:

Introduction

The **File** menu in Fabric Manager provides basic administrative options to the user. Table A-1 describes the options in the **File** menu.

Table A-1 File Menu Options

Option	Description
New...	Opens a new Fabric Manager window. All other Fabric Manager windows remain open.
Close	Closes the active Fabric Manager window. This option is only available when you open multiple Fabric Manager windows.
Fabric Login...	Opens the **Fabric Login** window to log in to multiple switches. For more information, refer to *Fabric Login Window* on page A-3.
Groups	Opens the **Groups** submenu so you can create, edit, import, and export switchgroups and portgroups. For more information on the **Groups** submenu, refer to *Groups Submenu* on page A-4. For information on how to create, edit, and delete groups, refer to Chapter 6, *Grouping*.
Options	Opens the **Options** window to set default options for the following areas: ◆ Topology ◆ Fabric Change ◆ ISL Status ◆ Log Parameters ◆ File Transfers For more information, refer to *Options Window* on page A-8.
Log...	Opens the **Fabric Log** window to view Fabric Manager log entries. For more information, refer to *Fabric Log Window* on page A-17.
Print...	Opens the **Print** window to print a report summary or topology.
Print In One Page...	Opens the **Print** window to print a topology to one page.
Page Setup...	Opens the **Page Setup** window to configure print options.
Exit	Closes Fabric Manager.

Fabric Login Window

The **Fabric Login** window lets you log in to multiple switches simultaneously. Table A-2 describes the components of the window.

For instructions that explain how to perform a fabric login, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.

Table A-2 Fabric Login Window Components

Component	Description
User Id field	Accepts the user ID that you use to log into the switches.
Password field	Accepts the password that you use to log into the switches.
Name/IP/WWN radio buttons	Determine how the **SAN Elements** tab identifies switches. For more information, refer to *Select Identity* on page 4-9.
SAN Elements tab	Displays the fabrics, switches, and groups that you can log in to.
Filter tab	Filters elements based on alphanumeric text strings.
directional arrows	Add or remove switches from the **Selected Switches** field.
Selected Switches field	Displays the switches that you have chosen to log in to.
IP Address column	Displays the IP address of each switch in the **Selected Switches** field. Click the column header to list all switches in ascending or descending order by IP address.
Switch Name column	Displays the switch name of each switch in the **Selected Switches** field. Click the column header to list all switches in ascending or descending order by switch name.
Firmware version column	Displays the firmware that runs on each switch in the **Selected Switches** field. Click the column header to list all switches in ascending or descending order by firmware version.
UserID column	Displays the user ID that you used to log in to each switch in the **Selected Switches** field. If you have not logged in to the switch, this field remains blank. Click the column header to list all switches in ascending or descending order by user ID.

Table A-2 Fabric Login Window Components (continued)

Component	Description
Status column	Displays the log in status of each switch in the **Selected Switches** field. Click the column header to list all switches in ascending or descending order by status.
Apply button	Applies the user ID and password that you specify to log in to one or more switches.
Close button	Closes the **Fabric Login** window.
Help button	Opens Fabric Manager Help.

Groups Submenu

The **Groups** submenu lets you configure, import, and export Fabric Manager logical groups. Table A-3 lists the options in this submenu and describes each option.

For instructions on how to create and edit logical groups, refer to Chapter 6, *Grouping*.

Table A-3 Groups Submenu Items

Option	Description
Edit Switch Groups...	Opens the **Edit Switch Groups** window to create or modify switch groups. For information on the window, refer to *Edit Switch Groups Window* on page A-5.
Edit Port Groups...	Opens the **Edit Port Groups** window to create or modify port groups. For information on the window, refer to *Edit Port Groups Window* on page A-5.
Import Group...	Opens the **Import from file** window to add a group (from a previously-saved group file) to your user profile. For instructions on how to import a group, refer to *Import a Group* on page 6-7.
Export Group...	Opens the **Export** window to export one or of the groups that you defined in Fabric Manager. For information on the window, refer to *Export Window* on page A-7.

Edit Switch Groups Window

The **Edit Switch Groups** window lets you create new switch groups and modify or delete existing switch groups. Table A-4 lists and describes the components of the window.

Table A-4 Edit Switch Groups Window Components

Component	Description
Name/IP/WWN radio buttons	Determine how the **SAN Elements** tab identifies switches. For more information, refer to *Select Identity* on page 4-9.
SAN Elements tab	Displays the fabrics and switches that you can add to your groups.
Filter tab	Filters elements based on alphanumeric text strings.
SwitchGroups navigation tree	Displays existing switch groups and lets you move groups within the tree.
Create... button	Opens the **Create Group** window to create and name a new switch group.
Edit... button	Opens the **Edit Group** window to rename an existing switch group.
Delete button	Deletes an existing switch group.
OK button	Applies and saves switch group edits.
Cancel button	Aborts switch group edits.
Help button	Opens **Fabric Manager Help** to the **Groups** section.

Edit Port Groups Window

The **Edit Port Groups** window lets you create new port groups and modify or delete existing port groups. Table A-5 lists and describes the components of the window.

Table A-5 Edit Port Groups Window Components

Component	Description
Name/IP/WWN radio buttons	Determine how the **SAN Elements** tab identifies switches. For more information, refer to *Select Identity* on page 4-9.
SAN Elements tab	Displays the fabrics and switches that you can add to your groups.
Filter tab	Filters elements based on alphanumeric text strings.
PortGroups navigation tree	Displays existing port groups and lets you move groups within the tree.
Create... button	Opens the **Create Group** window to create and name a new port group.
Edit... button	Opens the **Edit Group** window to rename an existing port group.
Delete button	Deletes an existing port group.
OK button	Applies and saves port group edits.
Cancel button	Aborts port group edits.
Help button	Opens **Fabric Manager Help** to the **Groups** section.

Export Window

Use the **Export** window to export one or more logical groups to a XML file. Table A-6 lists and describes the components of the window.

For instructions on how to export groups, refer to *Export Groups* on page 6-6.

Table A-6 Export Window Components

Component	Description
File field	Accepts the path to a file to which you export your group(s).
Browse... button	Opens the **Export to file** window to choose the file to which you export your group(s).
Name/IP/WWN radio buttons	Determine how the **SAN Elements** tab identifies switches. For more information, refer to *Select Identity* on page 4-9.
SAN Elements tab	Displays the fabrics and switches that you can add to your groups.
To Export field	Lists the groups to export.
Group column	Lists the name of each group in the **To Export** field.
Path column	Lists the path of each group in the **To Export** field. The path matches the hierarchy in the groups navigation tree.
Type column	Lists the group type (switch or port) of each group in the **To Export** field.
Save button	Saves groups to a file.
Cancel button	Aborts the export process.
Delete button	Removes one or more groups that you select from the **To Export** field.
Help button	Opens **Fabric Manager Help** to the **Groups** section.

Options Window

The **Options** window lets you configure various Fabric Manager defaults. The **Configurations** navigation tree displays the categories of options that you can configure. It is displayed in Figure A-1.

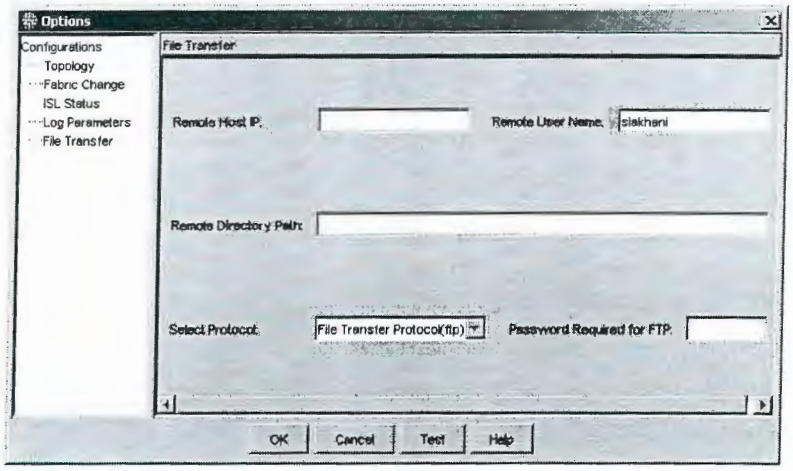


Figure A-1 Configurations Navigation Tree

Table A-7 lists and describes the categories of options that you can configure.

Table A-7 Options Categories

Category	Description
Topology	Lets you configure the following defaults: ◆ Default Startup Layout ◆ Default Startup Link Style ◆ Tile Direction ◆ Threshold Percent ◆ Threshold Trigger Period For more information on these defaults, refer to *Topology Options* on page A-11.
Fabric Change	Lets you configure the following: ◆ Fabric Checking ◆ Fabric Change handling For more information on these defaults, refer to *Fabric Change Options* on page A-12.
ISL Status	Lets you configure the following: ◆ Incorporate Adds into Stamp ◆ Add Conflict Status ◆ Add Status ◆ Remove Status ◆ Remove Direct Connection Status ◆ Move Status For more information on these defaults, refer to *ISL Status Options* on page A-12.

Table A-7 Options Categories (continued)

Category	Description
Log Parameters	Lets you configure the following: ◆ Log Directory Path ◆ Fabric Manager Log Level ◆ File Log Level For more information on these defaults, refer to *Log Parameter Options* on page A-15.
File Transfer	Lets you configure the following: ◆ Remote Host IP ◆ Remote User Name ◆ Remote Directory Path ◆ Select Protocol ◆ Password Required for FTP For more information on these defaults, refer to *File Transfer Options* on page A-16.

Topology Options

Configure topology options to establish the default appearance of fabric topologies in Topology view. Table A-8 lists and describes the default topology traits that you can configure.

Table A-8 Topology Options

Option	Description
Default Startup Layout pull-down menu	Configures the topology layout that appears by default when you open Topology view. You can select from the following layouts: ◆ **Circular** layout arranges the switches and nodes of a fabric into a circle. ◆ **Core-Edge** layout visually separates core switches, edge switches, and nodes. ◆ **Tree** layout organizes the fabric hierarchically. For more information on topology layouts, refer to *Topology View* on page C-23.
Default Startup Link Style pull-down menu	Configures the link style that appears by default when you open Topology view. You can select from the following styles: ◆ **Orthogonal** style displays all links as horizontal and vertical lines that turn at right angles. ◆ **Straight** style displays all links as straight, unbending lines that connect switches along the shortest path.
Tile Direction pull-down menu	Designates the way you want nonconnected graph objects to appear in relation to each other (horizontally or vertically).
Threshold Percent field	Configures the percent of bandwidth above which the link raises a flag.
Threshold Trigger Period field	Configures the amount of time (in seconds) that the bandwidth of a link must exceed the threshold percent before the link raises a flag. You cannot configure this field to a value higher than 60 seconds.
OK button	Applies configuration changes.
Cancel button	Aborts configuration changes.

Fabric Change Options

Configure fabric change options to enable and customize Fabric Checking. Table A-9 lists and describes the fabric change options that you can configure.

Table A-9 Fabric Change Options

Options	Description
Automatically check fabrics? checkbox	Enables fabric checking on all fabrics currently monitored by Fabric Manager, and any additional fabrics discovered from this point on. For more information on how to configure Fabric Checking, refer to *Automatically Enable Fabric Checking on All Fabrics* on page 14-5.
Fabric Change handling pull-down menu	Configures allowable changes to the fabric. Choose one of the following: ◆ Check for lost and added switches. ◆ Check for lost switches only.
OK button	Applies configuration changes.
Cancel button	Aborts configuration changes.

ISL Status Options

Configure ISL status options to establish:

- If Fabric Manager incorporates new switches directly into the stamp.
- The severity level of the flag that each status change evokes.

Table A-10 lists and describes the ISL status options that you can configure.

For instructions on how to configure ISL status parameters, refer to *Assign Color Status Settings* on page 13-3.

Table A-10 **ISL Status Options**

Options	Description
Incorporate Adds into Stamp checkbox	Automatically updates the ISL stamp when you add ISLs to the fabric.
Add Conflict Status radio buttons	Configures the color of the flag (red or yellow) that Fabric Manager raises when you connect an ISL to a port that, according to the stamp, "belongs" to a different switch in the fabric.
Add Status radio buttons	Configure the color of the flag (red or yellow) that Fabric Manager raises when you add an ISL that does not appear in the current stamp. You cannot configure this option if you select the **Incorporate Adds into Stamp** checkbox.

Table A-10 ISL Status Options (continued)

Options	Description
Remove Status radio buttons	Configure the color of the flag (red or yellow) that Fabric Manager raises when you remove an ISL that appears in the current stamp. You cannot configure Remove status to be more severe than Remove Direct Connection status.
Remove Direct Connection Status radio buttons	Configure the color of the flag (red or yellow) that Fabric Manager raises when you remove every link between two domains. Direct connect remove events occur when you remove every link between two domains/switches.
Move Status radio buttons	Configure the color of the flag (red or yellow) that Fabric Manager raises when you move an ISL from one port to another port on the same switch. Move events occur when you move one end of an ISL to a different port on the same switch, but do not change the port on the other end of the ISL.

Log Parameter Options

Configure log parameters to assign severity levels to various fabric events and to assign a directory to store logs. Table A-11 lists and describes log parameter options.

For instructions on how to configure log parameters, refer to *Configure Log Parameters* on page 4-12.

Table A-11 Log Parameter Options

Option	Description
Log Directory Path field	Configures the directory to which Fabric Manager stores logs.
Browse button	Opens the **Select** window to choose a directory to store logs.
Fabric Manager Log Level pulldown menu	Assigns the severity level of Fabric Manager application log entries.
File Log Level pull-down menu	Assigns the severity level of file log entries.
OK button	Applies log parameter changes.
Cancel button	Aborts log parameter changes.
Restore to Defaults button	Restores all fields to default values.
Help button	Opens Fabric Manager Help.

File Transfer Options

Configure file transfer options to perform tasks such as firmware download that require FTP to execute. Table A-12 lists and describes the file transfer fields.

For instructions on how to configure transfer options, refer to *Configure File Transfer Options* on page 4-16.

Table A-12 File Transfer Options

Option	Description
Remote Host IP field	Accepts the IP address of a host that runs FTP.
Remote User Name field	Accepts the username with which to log in to the host.
Remote Directory Path field	Accepts the path on the server to access.
Select Protocol pull-down menu	Identifies the protocol to use to contact the host.
Password Required for FTP field	Accepts the password with which to log in to the host.
OK button	Applies file transfer changes.
Cancel button	Aborts file transfer changes.
Test button	Tests if you can successfully access the host with the protocol you configured in the **Select Protocol** pulldown menu.
Help button	Opens Fabric Manager Help.

Fabric Log Window

The **Fabric Log** window lists log entries that the application logs about itself as it runs. This log appears for customer support purposes only. Table A-13 lists and describes the components of this window.

Table A-13 Fabric Log Components

Component	Description
Severity column	Displays the severity of the event that prompted the log entry. Click the column header to list all log entries in ascending or descending order by severity.
Time column	Displays the date and time that event occurred. Click the column header to list all log entries in ascending or descending order by time stamp.
Module column	Displays the application module associated with the event. Click the column header to list all log entries in ascending or descending order by module.
Message column	Displays messages for customer support. Click the column header to list all log entries in ascending or descending order by message.
Module Instance column	Displays Fabric Manager thread instances. Click the column header to list all log entries in ascending or descending order by application-module instance.
Detail Log Message window	Aggregates a row in the **Fabric Log** table into a single consolidated message.
Search button	Opens the **Search Dialog** window. For more information on this window, refer to *Search Dialog Window* on page A-17.
Filter button	Opens the **Filter Dialog** window. For more information on this window, refer to *Filter Dialog Window* on page A-19.
Close button	Closes the **Fabric Log** window.

Search Dialog Window

Use the **Search Dialog** window to search the contents of the log. Table A-14 lists and describes the components of the window.

Table A-14 Search Dialog Window Components

Component	Description
Message Contains field	Accepts text to search for in the message.
Case Sensitive checkbox	Applies case sensitivity when Fabric Manager searches for the text in the **Message Contains** field.
Severity pull-down menu	Limits the search to messages of particular severity levels.
Module field	Limits the search to messages with particular modules.
Date Range pull-down menus	Limits the search to messages with time stamps between a particular range (inclusive).
Search button	Begins the search.
Next button	Progresses to the next log entry that meets the search criteria.
Prev button	Returns to the previous entry that met the search criteria.
Close button	Closes the **Search Dialog** window.

Filter Dialog Window

Use the **Filter Dialog** window to filter the log entries that the **Fabric Log** window displays. Table A-15 lists and describes the components of the window.

The filter excludes all messages that do not meet the criteria of the **Filter Dialog** window.

For instructions on how to filter fabric events, refer to *Filter Events* on page 20-2.

Table A-15 Filter Dialog Window Components

Component	Description
Message Contains field	Accepts text that Fabric Manager uses as a criteria to filter out a message. Fabric Manager excludes all messages that do not contain the text.
Case Sensitive checkbox	Applies case sensitivity when Fabric Manager filters messages with the **Message Contains** field.
Severity pull-down menu	Filters out messages of all other severity levels.
Module field	Filters out messages of all other modules.
Date Range pull-down menus	Filters out all messages with dates that do not fall within the date range.
Filter button	Applies the filter.
Close button	Closes the **Filter Dialog** window.

2226
Paula

B

Edit Menu Reference

This appendix contains the following sections:

Introduction

The **Edit** menu manages elements of the GUI. Table B-1 describes the options in the **Edit** menu.

Table B-1 Edit Menu Options

Option	Description
Copy Table	Copies a table so you can paste it into an application that uses tab-delimited cell/return-delimited row format. To select the **Copy Table** option, you must first open one of the following views: ◆ Devices view ◆ Portgrid view ◆ Ports view ◆ Switches view
Rename	Changes the identifier of a switch, port, or fabric in the **SAN Elements** tab. This option does not reconfigure the switch name. It only changes how the fabric or switch appears in Fabric Manager. To select the **Rename** option, you must first click one of the following elements: ◆ A fabric in the **SAN Elements** tab ◆ A switch in the **SAN Elements** tab ◆ A port in the **SAN Elements** tab

Table B-1 Edit Menu Options (continued)

Option	Description
View Options...	Opens the **Edit View Options for** *X* window (where *X* represents the current active view) to customize the Fabric Manager display. For more information on this window, refer to *Edit View Options Windows* on page B-4.
Change description	Opens the **Please enter the new description** dialog box to change the description of a panel. Every Fabric Manager view that displays a panel (for instance, Summary view when you click **Fabrics** in the **SAN Elements** tab) includes a description. By default, this description reads **Double click to add description**. This option provides an alternative method to change the description. After you change the description of an element, you must click the parent element to view the new description in the panel.

Edit View Options Windows

Each view uses a different **Edit View Options** window, but not all views support the **Edit > View Options...** selection. You can open an **Edit View Options** window with the following views:

- Devices view
- Ports view
- Summary view (but only when you select a fabric, group, or switch from the **SAN Elements** tab)
- Switches view

The **Edit>View Options...** selection will be greyed out for all other views.

Edit View Options for Details

Details vary based on the element that you select in the **SAN Elements** tab. Table B-2 lists the elements that you can click in the **SAN Elements** tab and provides the window that opens. A description of each window follows the table.

Table B-2 Elements and Edit View Option Windows

Element	Window
My SAN	Not applicable. You cannot select **Edit > View Options...** when you click **My SAN**.
Fabrics	**Edit View Options for Fabric At-a-Glance Detail**
Any given fabric	**Edit View Options for Switch At-a-Glance Detail**
Any given switch	**Edit View Options for Card At-a-Glance Detail** (for switches that use cards) **Edit View Options for At-a-Glance Port Detail** (for all other switches)
Any given card	**Edit View Options for Port At-a-Glance Detail**
Any given port	**Edit View Options for Devices**
SwitchGroups	**Edit View Options for Logical Group At-A-Glance Detail**

Table B-2 Elements and Edit View Option Windows (continued)

Element	Window
any given switch group	**Edit View Options for Switch At-A-Glance Detail**
PortGroups	**Edit View Options for Port Group At-A-Glance Detail**
any given port group	**Edit View Options for Port At-A-Glance Detail**

Edit View Options for Fabrics At-A-Glance Detail

The **Edit View Options for Fabrics At-A-Glance Detail** window lists the various fabric traits and properties that Fabric Manager can display and lets you choose which options appear in Summary view. The **Edit View Options for Fabric Detail** window lets you choose from the following options:

- Launch switch
- Principal switch
- Member switches
- Switch status
- Switch types
- FabricOS versions
- Port information
- Device information
- Active zones

Edit View Options for Switch At-A-Glance Detail

The **Edit View Options for Switch At-A-Glance Detail** window lists the various switch traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. The **Edit View Options for Switch Detail** window lets you choose from the following options:

- Switch status
- Switch types
- Fabric OS versions
- Domain ID
- Ethernet IP
- Ethernet mask
- FCnet IP
- FCnet mask
- Gateway IP
- WWN
- Switch role
- Trunk information
- Member ports

- ISL ports
- Port status
- Port type
- Port speed
- Light state
- Port information
- Device information

Edit View Options for Card At-A-Glance Detail

The **Edit View Options for Card At-A-Glance Detail** window lists the various card traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. The **Edit View Options for Card Detail** window lets you choose from the following options:

- Member ports
- ISL ports
- Port status
- Port speed
- Light state
- Port information
- Device information

Edit View Options for Port At-A-Glance Detail

The **Edit View Options for Port At-A-Glance Detail** window lists the various port traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. The **Edit View Options for Port Detail** window lets you choose from the following options:

- Port number
- Port status
- Port type
- Port WWN
- Port speed
- Light state
- Device information

Edit View Options for Logical Group At-A-Glance Detail

The **Edit View Options for Logical Group At-A-Glance Detail** window lists the various switch group traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. The **Edit View Options for Logical Group Detail** window lets you choose from the following options:

- Groups information
- Member switches
- Switch status

- Switch types
- Fabric OS versions
- Port information
- Device information

Edit View Options for Port Group At-A-Glance Detail

The **Edit View Options for Port Group At-A-Glance** Detail window lists the various port traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. The **Edit View Options for Port Group Detail** window lets you choose from the following options:

- Groups information
- Member ports
- ISL ports
- Port status
- Port type
- Port speed
- Light state
- Port information
- Device information

Edit View Options for Devices

The **Edit View Options for Devices** window lists the various device traits and properties that Fabric Manager can display and lets you choose which options appear in Devices view. This window lets you choose from the following options:

- WWN
- SCSI Inquiry name
- Manufacturer
- Serial number
- Sequence number
- Model
- Model description
- Hardware
- Driver
- ROM version
- Firmware
- OS name and version
- Capability

Edit View Options for Ports

The **Edit View Options for Ports** window lists the various port traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Fabric
- Switch
- ID
- Status
- Light
- State
- Type
- Speed
- Port module
- Card number
- Port number
- User port number
- WWN
- Name

Edit View Options for Summaries

Summaries vary based on the element that you select in the **SAN Elements** tab. Table B-3 lists the elements that you can click in the **SAN Elements** tab and provides the window that opens. A description of each window follows the table.

Table B-3 Elements and Edit View Option Windows

Element	Window
My SAN	Not applicable. You cannot select **Edit > View Options...** when you click **My SAN**.
Fabrics	**Edit View Options for Fabric At-A-Glance Summary**
any given fabric	**Edit View Options for Switch At-A-Glance Summary**
any given switch	**Edit View Options for Card At-A-Glance Summary** (for switches that use cards) **Edit View Options for Port At-A-Glance Summary** (for all other switches)
any given card	**Edit View Options for Port At-A-Glance Summary**
any given port	**Edit View Options for Device At-A-Glance Summary**

Table B-3 Elements and Edit View Option Windows (continued)

Element	Window
SwitchGroups	**Edit View Options for Logical Group At-A-Glance Summary**
any given switch group	**Edit View Options for Switch At-A-Glance Summary**
PortGroups	**Edit View Options for Port Group At-A-Glance Summary**
any given port group	**Edit View Options for Port At-A-Glance Summary**

Edit View Options for Fabric At-A-Glance Summary

The **Edit View Options for Fabric At-A-Glance Summary** window lists the various fabric traits and properties that Fabric Manager can display and lets you choose which options appear in Summary view. This window lets you choose from the following options:

- Launch switch
- Principal switch
- Member switches
- Switch status
- Switch types
- FabricOS versions
- Port information
- Device information
- Active zones

Edit View Options for Switch At-A-Glance Summary

The **Edit View Options for Switch At-A-Glance Summary** window lists the various switch traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Switch status
- Switch types
- Fabric OS versions
- Domain ID
- Ethernet IP
- Ethernet mask
- FCnet IP
- FCnet mask
- Gateway IP
- WWN
- Switch role
- Trunk information
- Member ports

- ISL ports
- Port status
- Port type
- Port speed
- Light state
- Port information
- Device information

Edit View Options for Card At-A-Glance Summary

The **Edit View Options for Card At-A-Glance Summary** window lists the various card traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Blade state
- Power state
- Attn state
- Member ports
- ISL ports
- Port status
- Port type
- Port speed
- Light state
- Port information
- Device information

Edit View Options for Port At-A-Glance Summary

The **Edit View Options for Port At-A-Glance Summary** window lists the various port traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Port number
- Port status
- Port type
- Port WWN
- Port speed
- Light state
- Device information

Edit View Options for Logical Group At-A-Glance Summary

The **Edit View Options for Logical Group At-A-Glance Summary** window lists the various switch group traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Groups information
- Member switches
- Switch status
- Switch types
- Fabric OS versions
- Port information
- Device information

Edit View Options for Port Group At-A-Glance Summary

The **Edit View Options for Port Group At-A-Glance Summary** window lists the various port traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Groups information
- Member ports
- ISL ports
- Port status
- Port type
- Port speed
- Light state
- Port information
- Device information

Edit View Options for Switches

The **Edit View Options for Switches** window lists the various switch traits and properties that Fabric Manager can display and lets you choose which options appear in Ports view. This window lets you choose from the following options:

- Name
- IP
- Version
- Status
- Fabric
- ID
- IP mask
- Gateway
- FCIP
- FC mask

- Responding
- Role
- Domain ID
- WWN
- Serial number
- State
- Is core
- Port count
- Free Ports
- ISL count
- Secure mode
- Using FCIP
- Have UserID
- Has certificate
- Trunk count
- Trunked port count
- Device count
- Ficon mode (not supported in Fabric Manager V4.0)
- Switch part number

C View Menu Reference

This appendix contains the following sections:

Introduction

The **View** menu lists the various Fabric Manager views. The sections that follow describe each view. You can use the **View** menu to navigate Fabric Manager just as you use the view selector. For more information on the navigation options, refer to *Navigate with Elements and Views* on page 4-9.

Detail View

Detail view provides detailed information about SAN elements. When you click an element in the **SAN Elements** tab and select Detail view, Fabric Manager displays a panel for each nested element. (That is, if you click a fabric, you see panels for each switch in the fabric; if you click a switch, you see panels for each card or port on the switch.) You can expand any item in the panel that includes two right-angle brackets (>>). Click the item to expand it. Click the item again to collapse it.

My SAN Detail

Each panel in **My SAN Detail** provides an **At-A-Glance overview** of the major categories of elements: **Fabrics**, **SwitchGroups**, and **PortGroups**. The information that appears in the overview depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Devices* on page B-7.

Each **At-A-Glance overview** panel includes a series of icons at the bottom. The icons in the bottom-left corner of the panel represent the switch types (in the case of **SwitchGroups** and **Fabrics**) or port types (in the case of **PortGroups**) that appear in that element. One icon appears for each type of switch or port that appears. Place your pointer over the icon to display the number of that type of device that appears.

The icons that appear in the bottom-right corner of the **At-A-Glance overview** pane provide administrative options. Table C-1 presents and describes each icon.

Table C-1 At-A-Glance Overview Administrative Icons

Icon	Description
Events icon ( )	Opens Event view in a new Fabric Manager window for the appropriate element. (For instance, if you click the **events** icon in the **SwitchGroups** pane, Fabric Manager selects **SwitchGroups** from the **SAN Elements** tab and opens Event view.) For more information, refer to *Event View* on page C-10.
Display icon ( )	Opens the **Edit View Options** window for the appropriate element. For more information, refer to *Edit View Options Windows* on page B-4.
Update icon ( )	Updates the information in the display pane.

Fabrics Detail

Each pane in the **Fabrics Detail** view displays details about each fabric. The information that appears in the overview depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each pane includes a series of icons at the bottom. The icons in the bottom-left corner of the pane represent the switch types that appear in the fabric. One icon appears for each type of switch that appears in the fabric. Place your pointer over the icon to see how many switches of that type appear in the fabric.

The icons that appear in the bottom-right corner of the pane provide administrative options. Table C-2 presents and describes each icon.

Table C-2 Fabrics Detail Icons

Icon	Description
Fabric Events icon ( )	Opens Event view in a new Fabric Manager window for the appropriate fabric. (For instance, if you click the **Fabric Events** icon in the **Switch** *X* panel, Fabric Manager selects Switch *X* from the **SAN Elements** tab and opens Event view.) For more information, refer to *Event View* on page C-10.
Zone Admin icon ( )	Opens the **Zone Admin** windows of Web Tools.
Name Server icon ( )	Opens the **Name Server Table** window of Web Tools.

Table C-2 Fabrics Detail Icons (continued)

Icon	Description
Fabric Topology icon	Opens Web Tools Topology view to show tables of data that display the routes that the data takes.
Security Admin con	Opens the **Security Admin** window. For more information, refer to Chapter 10, *Security Management*. This icon only appears in the pane of a secure fabric.
Telnet to FCS icon	Opens a Telnet session to the FCS. For more information, refer to Chapter 10, *Security Management*. This icon only appears in the pane of a secure fabric.
Update icon	Updates the information in the display pane.

Miscellaneous Fabric Detail

Each panel in the detail view of a given fabric displays details about a switch in the fabric. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each pane represent the port types that appear in the switch. One icon appears for each type of port that appears in the switch. Place your pointer over the icon to see how many ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-3 presents and describes each icon.

Table C-3 Misc. Fabric Detail Icons

Icon	Description
Switch Events icon ( )	Opens Event view for the switch in a new Fabric Manager window.
Admin View icon ( )	Opens the **Switch Admin** window of Web Tools.
Fabric Watch icon ( )	Opens the **Fabric Watch** window of Web Tools.
Telnet icon ( )	Opens a Telnet session to the switch.
Update icon ( )	Updates the information in the display pane.

Miscellaneous Switch Detail

Each panel in the detail view of a given switch displays details about a card or port in the switch. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

For switches that use cards, each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each panel represent the port types that appear in the switch. One icon appears for each type of port that appears in the switch. Place your pointer over the icon to see how many cards or ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-4 presents and describes each icon.

Table C-4 Misc. Switch Detail Icons

Icon	Description
Update icon ( )	Updates the information in the display pane.

Miscellaneous Card Detail

Each panel in the detail view of a given card displays details about a port in the card. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-5 presents and describes each icon.

Table C-5 **Misc. Card Detail Icons**

Icon	Description
Update icon ( )	Updates the information in the display pane.

SwitchGroups Detail

Each panel in the **SwitchGroups Detail** view displays details about a particular switch group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each pane represent the switch types that appear in the group. One icon appears for each type of switch that appears in the group. Place your pointer over the icon to see how many switches of that type appear in the group.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-6 presents and describes each icon.

Table C-6 **SwitchGroups Detail Icons**

Icon	Description
Group Events icon ( )	Opens Event view for the switch in a new Fabric Manager window.
Group Creation icon ( )	Opens the **Edit Switch Group** window. For more information on this window, refer to *Edit Switch Groups Window* on page A-5.
Group Exportation icon ( )	Opens the **Export** window. For more information on this window, refer to *Export Window* on page A-7.
Update icon ( )	Updates the information in the display pane.

Miscellaneous Switch Group Detail

Each panel in the detail view of a given switch group displays details about a switch in the group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each pane represent the port types that appear in the switch. One icon appears for each type of port that appears in the switch. Place your pointer over the icon to see how many ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-7 presents and describes each icon.

Table C-7 Misc. Switch Group Detail Icons

Icon	Description
Switch Events icon ( )	Opens Event view for the switch in a new Fabric Manager window.
Admin View icon ( )	Opens the **Switch Admin** window of Web Tools.
Fabric Watch icon ( )	Opens the **Fabric Watch** window of Web Tools.
Telnet icon ( )	Opens a Telnet session to the switch.
Update icon ( )	Updates the information in the display panel.

PortGroups Detail

Each panel in the **PortGroups Detail** view displays details about a particular port group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each panel represent the port types that appear in the group. One icon appears for each type of port that appears in the port group. Place your pointer over the icon to see how many ports of that type appear in the group.

The icons that appear in the bottom-right corner of the pane provide administrative options. Table C-8 presents and describes each icon.

Table C-8 PortGroups Detail Icons

Icon	Description
Group Creation icon ( )	Opens the **Edit Port Group** window. For more information on this window, refer to *Edit Port Groups Window* on page A-5.
Group Exportation icon ( )	Opens the **Export** window. For more information on this window, refer to *Export Window* on page A-7.
Update icon ( )	Updates the information in the display pane.

Miscellaneous Port Group Detail

Each pane in the detail view of a given port group displays details about a port in the group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

The icons that appear in the bottom-right corner of the pane provide administrative options. Table C-9 presents and describes each icon.

Table C-9 Misc. Port Group Detail Icons

Icon	Description
Update icon ( )	Updates the information in the display pane.

Devices View

Devices view lists the devices attached to a given element in the **SAN Elements** tab. The properties that Devices view displays appear in Table C-10.

Table C-10 Devices View Display

Column	Description
WWN	The World Wide Name of the device.
SCSI Inquiry Name	The SCSI inquiry name of the device. The SCSI inquiry name serves as the symbolic SCSI name of the device. If the device does not have a SCSI inquiry name, nothing appears in this field.
Manufacturer	The manufacturer of FDMI-capable devices.
Serial number	The serial number of FDMI-capable HBAs.
Model	The model descriptor of FDMI-capable HBAs.
Model Description	A description of an FDMI-capable device.
Hardware	An internal identifier of the FDMI-capable HBA manufacturer.
Driver	The driver that host runs for that HBA.
ROM version	The ROM version.
Firmware	The firmware that the HBA runs.
OS name and version	The OS of the device on which the HBA is installed.
Capability	The capability.

Event View

Event view consists of two sections, as follows:

- Current Status Reason
- Event Log

Event view is displayed in Figure C-1.

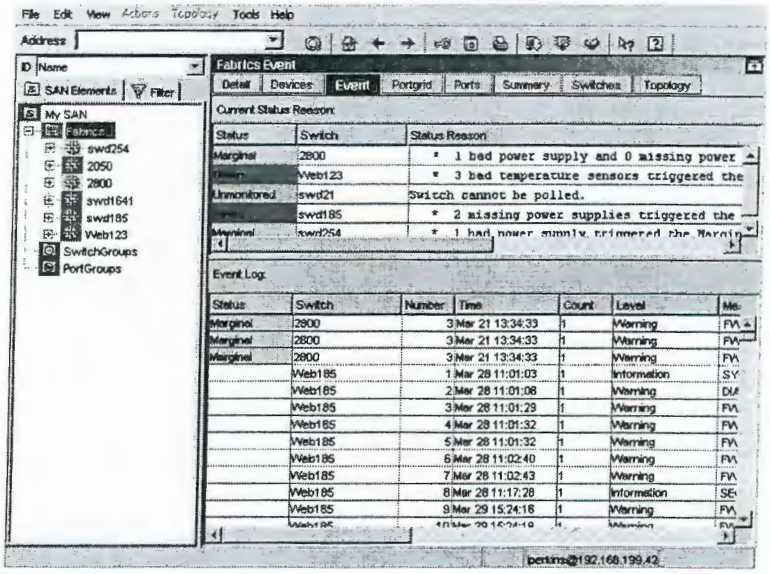


Figure C-1 **Event View**

The Current Status Reason section provides the following information about each switch that appears:

- the status of the switch
- the name of the switch
- the reason for the state of the switch

The Event Log section lists log entries and provides information about each entry. Table C-11 describes the information that appears in each entry.

Table C-11 Event View Log Entry Display

Property	Description
Status	The status of the switch.
Switch	The name of the switch.
Number	The number of the event. Events are numbered sequentially based on the time that they occurred.
Time	The time that the event occurred.
Count	The number of consecutive occurrences of the same event.
Level	The severity level of the event.
Message	The description of the event that occurred. Fabric Manager takes this description from the error log of the switch.
EventSrc	The event source, such as a daemon or library module. The possible event sources are: ◆ BLADE ◆ BLOOM ◆ DIAG ◆ EM ◆ ERRLOG ◆ FABRIC ◆ FICON (not supported in Fabric Manager V4.0) ◆ FSSME ◆ FW ◆ HAM ◆ HAMKERNEL ◆ MS ◆ PD TRACE ◆ RCS ◆ SULIB ◆ SYSC ◆ TRACK ◆ TS ◆ ZONE ◆ kSWD ◆ syslog

The quantity of switch and log information depends on the item that you choose from the **SAN Elements** tab.

Portgrid View

Portgrid view displays which ports connect to which devices for switches. Portgrid view only works when you click **My SAN**, **Fabrics**, or a specific fabric or switch in the **SAN Elements** tab. If a device has a SCSI inquiry name, Portgrid view will display it. If not, Portgrid view will display the WWN. For loop devices, Portgrid view shows `loop` and the number of devices in the loop.

Ports View

Ports view provides detailed information on every port in the element you select from the **SAN Elements** tab. The view includes status information. The following events (and only these events) change the port status to *down*:

- Diag_Flt
- Lock_Ref
- Port_Flt
- No_Sync
- Laser_Flt
- No_Port

The following events (and only these events) change the port status to *marginal*:

- No_Light
- Disabled
- Testing

The following events (and only these events) change the port status to *healthy*:

- In_Sync
- No_Module
- No_Card
- Online

Table C-12 describes the details that appear in Ports view.

Table C-12 Ports View Display

Property	Description
Fabric	The name of the fabric to which the port belongs.
Switch	The name of the switch to which the port belongs.
ID	The port ID of the port.
Status	The status of the port.
Light	The LED state of the port.
State	The state of the port module.
Type	The port type of the port.
Speed	The speed of the port in gbit/sec.
Port Module	Whether the port is copper or fiber.
Card Number	The card in a dual-switch chassis to which the port belongs.
Port Number	The number of the port in the port card (0-15).
User Port Number	The number of the port in the switch (variable).
WWN	The WWN of the port.
Name	The name that you assigned to the switch with Fabric Manager. For more information, refer to *Rename a Port* on page 4-6.
Responding	The current responding state of the HTTP session.

Summary View

Summary view provides high-level information about SAN elements. When you click an element in the **SAN Elements** tab and select Summary view, Fabric Manager displays a panel for each nested element. (That is, if you click a fabric, you see panels for each switch in the fabric; if you click a switch, you see panels for each card or port on the switch.) You can expand any item in the panel that includes two right angle brackets (>>). Click the item to expand it. Click the item again to collapse it.

My SAN Summary

Each panel in **My SAN Summary** provides an **At-A-Glance overview** of the major categories of elements: **Fabrics**, **SwitchGroups**, and **PortGroups**. The information that appears in the overview depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Devices* on page B-7.

Each **At-A-Glance overview** panel includes a series of icons at the bottom. The icons in the bottom-left corner of the panel represent the switch types (in the case of **SwitchGroups** and **Fabrics**) or port types (in the case of **PortGroups**) that appear in that element. One icon appears for each type of switch or port that appears. Place your pointer over the icon to display the number of that type of device that appears.

The icons that appear in the bottom-right corner of the **At-A-Glance overview** panel provide administrative options. Table C-13 presents and describes each icon.

Table C-13 At-A-Glance Overview Administrative Icons

Icon	Description
Events icon ( )	Opens Event view in a new Fabric Manager window for the appropriate element. (For instance, if you click the **Events** icon in the **SwitchGroups** panel, Fabric Manager selects **SwitchGroups** from the **SAN Elements** tab and opens Event view.) For more information, refer to *Event View* on page C-10.
Display icon ( )	Opens the **Edit View Options** window for the appropriate element. For more information, refer to *Edit View Options Windows* on page B-4.
Update icon ( )	Updates the information in the display panel.

Fabrics Summary

Each panel in the **Fabrics Summary** view displays details about each fabric. The information that appears in the overview depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of the panel represent the switch types that appear in the fabric. One icon appears for each type of switch that appears in the fabric. Place your pointer over the icon to see how many switches of that type appear in the fabric.

The icons that appear in the bottom-right-hand corner of the panel provide administrative options. Table C-14 presents and describes each icon.

Table C-14 Fabrics Detail Icons

Icon	Description
Fabric Events icon ( )	Opens Event view in a new Fabric Manager window for the appropriate fabric. (For instance, if you click the **Fabric Events** icon in the **Switch** *X* panel, Fabric Manager selects Switch *X* from the **SAN Elements** tab and opens Event view.) For more information, refer to *Event View* on page C-10.
Zone Admin icon ( )	Opens the **Zone Admin** windows of Web Tools.
Name Server icon ( )	Opens the **Name Server Table** window of Web Tools.
Fabric Topology icon ( )	Opens Web Tools topology view to show tables of data that display the routes that the data takes.
Security Admin con ( )	Opens the **Security Admin** window. For more information, refer to Chapter 10, *Security Management*. This icon only appears in the panel of a secure fabric.
Telnet to FCS icon ( )	Opens a Telnet session to the FCS. For more information, refer to Chapter 10, *Security Management*. This icon only appears in the pane of a secure fabric.
Update icon ( )	Updates the information in the display panel.

Miscellaneous Fabric Summary

Each panel in the Summary view of a given fabric displays summary information about a switch in the fabric. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each pane represent the port types that appear in the switch. One icon appears for each type of port that appears in

the switch. Place your pointer over the icon to see how many ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-15 presents and describes each icon.

Table C-15 Misc. Fabric Detail Icons

Icon	Description
Switch Events icon ( )	Opens Event view for the switch in a new Fabric Manager window.
Admin View icon ( )	Opens the **Switch Admin** window of Web Tools.
Fabric Watch icon ( )	Opens the **Fabric Watch** window of Web Tools.
Telnet icon ( )	Opens a Telnet session to the switch.
Update icon ( )	Updates the information in the display panel.

Miscellaneous Switch Summary

Each panel in the summary view of a given switch displays summary information about a card or port in the switch. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

For switches that use cards, each panel includes a series of icons at the bottom. The icons in the bottom-left-hand corner of each panel represent the card or port types that appear in the switch. One icon appears for each type of port that appears in the switch. Place your pointer over the icon to see how many cards or ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-16 presents and describes each icon.

Table C-16 Misc. Switch Detail Icons

Icon	Description
Update icon ( )	Updates the information in the display panel.

Miscellaneous Card Summary

Each panel in the Summary view of a given card displays summary information about a port in the card. The information that appears depends on the options that you configure with the **Edit** menu. For

more information on view options, refer to *Edit View Options Windows* on page B-4.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-17 presents and describes each icon.

Table C-17 Misc. Card Detail Icons

Icon	Description
Update icon ( )	Updates the information in the display panel.

SwitchGroups Summary

Each panel in the **SwitchGroups Summary** view displays summary information about a particular switch group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each panel represent the switch types that appear in the group. One icon appears for each type of switch that appears in the group. Place your pointer over the icon to see how many cards or ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-18 presents and describes each icon.

Table C-18 SwitchGroups Detail Icons

Icon	Description
Group Events icon ( )	Opens Event view for the switch in a new Fabric Manager window.
Group Creation icon ( )	Opens the **Edit Switch Group** window. For more information on this window, refer to *Edit Switch Groups Window* on page A-5.
Group Exportation icon ( )	Opens the **Export** window. For more information on this window, refer to *Export Window* on page A-7.
Update icon ( )	Updates the information in the display panel.

Miscellaneous Switch Group Summary

Each panel in the summary view of a given switch group displays summary information about a switch in the group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each panel represent the port types that appear in the switch. One icon appears for each type of port that appears in the switch. Place your pointer over the icon to see how many ports of that type appear in the switch.

The icons that appear in the bottom-right corner of the panel provide administrative options. Table C-19 presents and describes each icon.

Table C-19 Misc. Switch Group Detail Icons

Icon	Description
Switch Events icon ( )	Opens Event view for the switch in a new Fabric Manager window.
Admin View icon ( )	Opens the **Switch Admin** window of Web Tools.
Fabric Watch icon ( )	Opens the **Fabric Watch** window of Web Tools.
Telnet icon ( )	Opens a Telnet session to the switch.
Update icon ( )	Updates the information in the display panel.

PortGroups Summary

Each panel in the **PortGroups Summary** view displays summary information about a particular port group. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

Each panel includes a series of icons at the bottom. The icons in the bottom-left corner of each panel represent the port types that appear in the group. One icon appears for each type of port that appears in the port group. Place your pointer over the icon to see how many ports of that type appear in the group.

The icons that appear in the bottom-right-hand corner of the panel provide administrative options. Table C-20 presents and describes each icon.

Table C-20 PortGroups Detail Icons

Icon	Description
Group Creation icon ( )	Opens the Edit Port Group window. For more information on this window, refer to *Edit Port Groups Window* on page A-5.
Group Exportation icon ( )	Opens the **Export** window. For more information on this window, refer to *Export Window* on page A-7.
Update icon ( )	Updates the information in the display panel.

Miscellaneous Port Group Summary

Each panel in the detail view of a given port group displays details about a port in the port. The information that appears depends on the options that you configure with the **Edit** menu. For more information on view options, refer to *Edit View Options for Summaries* on page B-8.

The icons that appear in the bottom-right-hand corner of the panel provide administrative options. Table C-21 presents and describes each icon.

Table C-21 Misc. Port Group Detail Icons

Icon	Description
Update icon ( )	Updates the information in the display panel.

Switches View

Table C-22 describes the information that Switches view displays about switches.

Table C-22 Switches View Display

Property	Description
Name	The name of the switch.
IP	The IP address of the switch.
Version	The firmware version that the switch runs.
Status	The status of the switch.
Fabric	The fabric to which the switch connects.
ID	The ID that you choose from the **ID** pull-down menu. For more, refer to *Select Identity* on page 4-9.
IP Mask	The subnet mask of the switch.
Gateway	The gateway of the switch.
FCIP address	The FCIP address of the switch, if configured.
FC Mask	The FC mask of the switch, if configured.
Responding	**True** if the switch responds to Fabric Manager, **false** if it does not.
Role	The role that the switch plays in the fabric (principal or subordinate).
Domain ID	The domain ID of the switch.
WWN	The WWN of the switch.
Serial Number	The serial number of the switch.
State	Whether the switch is enabled or disabled.
Is Core	Whether the switch is a core switch or an edge switch. For more information, refer to *Designate a Switch as a Core Switch* on page 4-19.
Port Count	The number of ports in the switch.
Free Ports	The number of unused/available ports in the switch.

Table C-22 Switches View Display (continued)

Property	Description
ISL Count	The number of ISLs that connect to the switch.
Secure Mode	Whether Secure Mode is enabled or disabled.
Using FCIP	Whether the switch is configured for FCIP.
Have UserID	Whether user information has been added to a switch. Provides fabric login (flogi) status.
Has Certificate	Whether a security certificate is installed.
Trunk Count	The number of trunks that connect to the switch.
Trunked Port Count	The number of ports in each trunk that connects to the switch.
Device Count	The number of devices that connect to the switch.
Ficon Mode	Whether the switch is operating in FICON mode. (Not supported in Fabric Manager V4.0.)
Switch PartNumber	The chassis part number, for applicable switches.

Figure C-2 displays Switches view as it appears when you click **My SAN** in the **SAN Elements** tab.

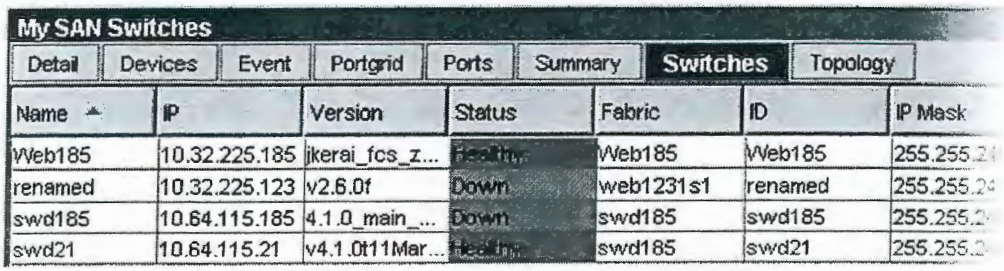


Figure C-2 Switches View

Topology View

Topology view provides a graphical representation of the elements that Fabric Manager monitors and the connections between and within them. When you open Topology view, a number of icons appear at the top of your Fabric Manager window. Table C-23 lists and describes these icons.

Topology view may take a considerable amount of time to open. Topology view options may also respond slowly.

Table C-23 Topology View Icons

Icon	Description
Pan icon ()	Lets you click and drag the Topology view to pan up, down, left, and right to see different portions of the view.
Select icon ()	Lets you move nodes in Topology view.
Zoom in rect icon ()	Lets you click and drag to zoom in on a particular rectangular region of the topology.
Zoom in icon ()	Zooms in.
Zoom out icon ()	Zooms out.
Fit to view icon ()	Resizes the entire topology to fit in your Fabric Manager window.
Overview icon ()	Opens a new window that displays the entire topology in miniature.
Snap Shot icon ()	Takes a screen shot of your topology graph that you can save in .png format.
Straight Link Style icon ()	Arranges links so they connect in a straight line from one element to another.
Orthogonal Link Style icon ()	Arranges links in horizontal and vertical lines, with right angles, to connect elements.

Topology view provides three different layout options: circular, core-edge, and tree. Table C-24 describes these layouts.

Table C-24 Topology View Layouts

Layout	Description
Circular	Arranges the switches and nodes of a fabric into a circle.
Core-edge	Separates core switches, edge switches, and nodes.
Tree	Organizes the fabric hierarchically.

Each Topology view consists of nested panes and element icons. Element icons that contain other elements (for instance, as a fabric contains switches) include an expand (+) icon in the top-left corner. If you expand the icon, the icon becomes a pane that displays the nested icons. Panes include a collapse icon (-) in the top-left corner so you can hide the subordinate icons.

Links

The lines that connect icons in Topology view represent different varieties of links in the fabrics. Table C-25 displays the various link images and explains the meaning of each.

Table C-25 Topology View Link Images

Image		Description
	bundled links	Represents all links between two switches to reduce clutter in the topology display. Double-click the bundle to expand it.
	expanded bundle	Displays the individual links that form a bundle. Double-click the expanded bundle to collapse the links into a bundle.
	1 Gb/s link	Represents a 1 Gb/s link between two switches. When you enable ISL Checking, this link appears as red, yellow, or green based on the ISL Checking status of the link. For more information, refer to *ISL Changes and Topology View* on page 13-6.

Table C-25 Topology View Link Images (continued)

Image		Description
	2 Gb/s link	Represents a 2 Gb/s link between two switches. When you enable ISL Checking, this link appears as red, yellow, or green based on the ISL Checking status of the link. For more information, refer to *ISL Changes and Topology View* on page 13-6.
	trunked links	Represents a trunk between two switches. This link appears as red, yellow, or green based on the ISL Checking status of the link.
	device groups	Represents the devices that connect to a switch. Double-click the device group to open a window that displays the devices in table format.
	device links	Represents the link between a switch and the devices that connect to it.

D

Actions Menu

This appendix includes the following sections:

Introduction

The **Actions** menu displays tasks that you can perform with Fabric Manager. You can only access items in this menu when you click one of the following in the **SAN Elements** tab:

- A specific fabric
- A specific switch
- A switch group node
- A switch group
- A specific port
- A port group node
- A port group
- A specific card (for switches that support cards)

Fabric Actions

When you click a fabric in the **SAN Elements** tab and open the **Actions** menu, the menu provides a series of fabric-wide tasks that you can perform. Table D-1 lists and describes the actions.

Table D-1 Fabric Actions

Action	Description
Events	Opens the Fabric Manager Event Log.
Telnet to FCS...	Telnets to the FCS of a secure fabric. If you click a nonsecure fabric in the **SAN Elements** tab, you cannot access this action and it appears as **Telnet...** This option only appears when you click a secure fabric in the **SAN Elements** tab.
Security...	Opens the **Security Admin** window to administer security. For more information, refer to *Security Admin Window* on page D-5. This option only appears when you click a secure fabric in the **SAN Elements** tab.
Zone Admin...	Opens the **Zone Administration** window of Web Tools.
Name Server...	Opens the **Name Server Table** window in Web Tools.
ISL	Opens the ISL submenu to initiate or restamp ISL Checking. For more information, refer to *ISL Submenu* on page D-7.
Set Time...	Opens the **Time** dialog box to update the time and date settings on the switches in the fabric. To configure the time, place your cursor in any part of the **Time** field and use the up arrow or down arrow to iterate the field; then click **OK**.
Refresh FDMI Info	Refreshes FDMI information. This option only appears when FDMI-capable HBAs are connected to switches running Fabric OS versions that support FDMI.

Table D-1 Fabric Actions (continued)

Action	Description
Backup...	Opens the **Backup fabric configuration-Select a folder** window to create a backup file that contains the following information: ◆ The configuration file of every switch in the fabric ◆ The license keys for every switch in the fabric ◆ A list of switches that belong to the fabric ◆ An ISL stamp The Backup action does not store the current ISL stamp. It creates a stamp of the ISLs as they appear *at the moment of the backup.* ◆ All zone definitions (and notes the active zone) ◆ Which firmware version each switch runs ◆ Name server information
Diff with Backup...	Opens the **Diff fabric configuration with backup** window to compare a fabric to a backup file and lists discrepancies.
Fabric Checking	Activates or deactivates Fabric Checking. A dark blue ring appears around the fabric icon to indicate that you enabled Fabric Checking, and a check mark appears next to the action in the **Actions** menu.
Refresh	Refreshes the Fabric Manager display to reflect any status changes.
Delete	Deletes the selected fabric.
Rename	Allows you to rename the selected fabric.

Security Admin Window

The **Security Admin** window consists of tabs that let you view and configure the various security policies. The **Security Admin** window is displayed in Figure D-1.

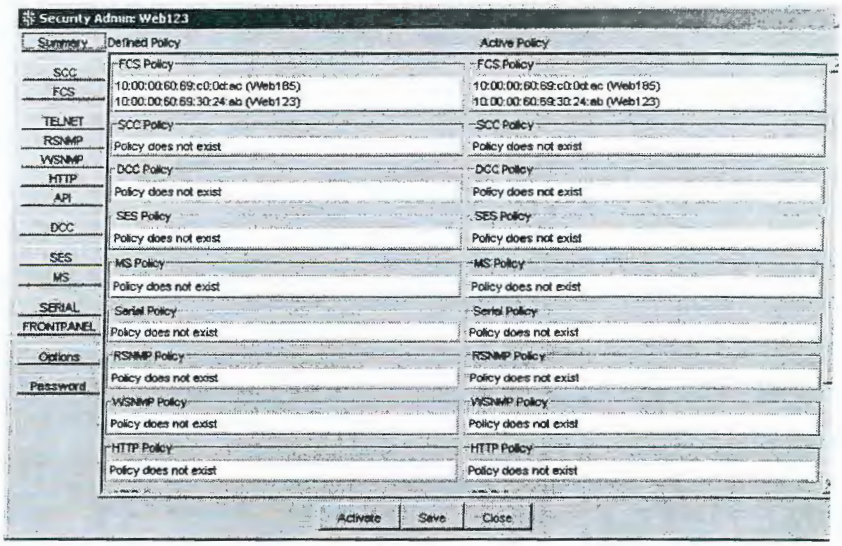


Figure D-1 Security Admin Window

Table D-2 lists and describes the tabs and buttons in the **Security Admin** window.

Table D-2 Security Admin Window Objects

Object	Description
Summary tab	Presents a column of defined security policies and a column of active security policies.
SCC tab	The components of this tab let you add a switch to a secure fabric. For more information, refer to *Add a Switch to a Secure Fabric* on page 10-5.
FCS tab	The components of this tab display each switch that serves as a Fabric Configuration Server (FCS) and lets you add or remove switches from the list.
TELNET tab	The components of this tab let you grant access to individual switches to run Telnet in a secure fabric.

Table D-2 Security Admin Window Objects (continued)

Object	Description
RSNMP tab	The components of this tab let you grant access to individual switches to run RSNMP in a secure fabric.
WSNMP tab	The components of this tab let you grant access to individual switches to run WSNMP in a secure fabric.
HTTP tab	The components of this tab let you grant access to individual switches to run HTTP in a secure fabric.
API tab	The components of this tab let you grant access to individual switches to run API in a secure fabric.
DCC tab	The components of this tab let you create a security policy. For more information, refer to *Configure DCC Policy Options* on page 10-13.
SES tab	The components of this tab let you grant access to individual switches to run SES in a secure fabric.
MS tab	The components of this tab let you grant access to individual switches to run Management Server in a secure fabric.
SERIAL tab	The components of this tab let you grant access to individual switches to accept a serial connection in a secure fabric.
FRONTPANEL tab	The components of this tab let you grant access to individual switches to accept configuration changes from the front panel in a secure fabric.
Options tab	The field in this tab lets you enable or disable No Node WWN zoning.
Password tab	The components of this tab let you change passwords for FCS switches and non-FCS switches.
Activate button	Activates the changes that you made to the components of the **Security Admin** window tabs.
Save button	Saves the changes that you made to the components of the **Security Admin** window tabs but does not apply them.
Close button	Closes the **Security Admin** window.

ISL Submenu

The **ISL** submenu lets you initiate or restamp ISL Checking. Table D-3 lists and describes the options that appear in the **ISL** submenu.

Table D-3 ISL Submenu Options

Option	Description
ISL Checking	Enables ISL Checking. For more information on this topic, refer to Chapter 13, *ISL Checking*.
Restamp	Resets the ISL stamp to which ISL Checking compares the fabric. For more information on this topic, refer to *Stamp/Restamp* on page 13-4.

Switch Actions

When you click a switch in the **SAN Elements** tab and open the **Actions** menu, the menu provides a series of switch-wide tasks that you can perform. Table D-4 lists and describes the actions.

Table D-4 Switch Actions

Action	Description
Events	Opens the Events View in Fabric Manager.
Switch View	Opens the **Switch View** window of Web Tools.
Admin...	Opens the **Switch Admin** window of Web Tools.
Fabric Watch...	Opens the **Fabric Watch** window of Web Tools.
Telnet	Opens a Telnet session to the switch.
Close Telnet	Closes a Telnet session to the switch. This option is not applicable to switches that run 4.X firmware.
Disable/Enable	Disables or enables the switch.

Table D-4 Switch Actions (continued)

Action	Description
Core Switch	Labels a switch as a core switch. This action impacts the location of the switch in Topology view for Core Edge layouts.
Delete	Deletes the switch.
Rename	Allows you to rename the switch.

Port Actions

When you click a port in the **SAN Elements** tab and open the **Actions** menu, the menu provides port-wide tasks that you can perform. Table D-5 lists and describes the actions.

Table D-5 Port Actions

Action	Description
Disable/Enable	Disables or enables the port.

E

Topology Menu Reference

This appendix includes the following sections:

Introduction

The **Topology** menu provides options to help you use and customize Topology view. You can only access the **Topology** menu after you open Topology view. Table E-1 lists and describes **Topology** menu options.

Fabric size impacts Topology view response speed.

Table E-1 Topology Menu Options

Option	Description
Layout	Opens the **Layout** submenu to select a layout or clear any changes you made to the layout. For more information on Topology view layouts, refer to *Topology View* on page C-23.
Links	Opens the **Links** submenu to: ◆ Expand all links ◆ Collapse all links ◆ Orthogonal link style ◆ Straight link style
Overview	Opens a new window that displays the entire topology in miniature.
Snapshot	Takes a snapshot of your current topology so you can compare a later topology to this baseline.

F

Tools Menu Reference

This appendix contains the following sections:

Introduction

The **Tools** menu serves as a toolbox of mini-applications to help you perform a variety of tasks. Table F-1 lists and describes the options in the **Tools** menu.

Table F-1 Tools Menu Options

Option	Description
Firmware download to switches...	Opens the **Firmware download to switches** window. For more information on how to download firmware to switches with Fabric Manager, refer to Chapter 12, *Firmware Download*.
Firmware download to HBAs...	Opens the **Firmware download to HBAs** window. For more information on how to download firmware to HBAs with Fabric Manager, refer to Chapter 19, *Emulex HBA Firmware Download*.
Reboot	Opens the **Reboot** submenu to configure or execute a sequenced reboot. For more information, refer to *Reboot Submenu* on page F-3.
Config	Opens the **Config** submenu to save a baseline configuration or to compare configurations. For more information, refer to *Config Submenu* on page F-4.
Licensing	Opens the **Licensing** submenu to manage software licenses. For more information, refer to *Licensing Submenu* on page F-5.
Fabric Merge...	Opens the **Fabric Merge Check** dialog box to verify that you can merge two fabrics successfully. For more information, refer to *Check Fabrics* on page 15-3.
Subnet scan...	Opens the **Subnet scan** dialog box to discover available fabrics.
Call Home	Opens the **Call Home** window. For more information, refer to Chapter 11, *Call Home*.

Reboot Submenu

The **Reboot** submenu helps you prepare and execute a sequenced reboot. Table F-2 lists and describes the options in this menu.

Table F-2 Reboot Submenu Options

Option	Description
Create Reboot Sequence...	Opens the **Create or change reboot groups and sequence** window to make or edit a reboot group. For more information on how to create and change reboot groups, refer to Chapter 18, *Sequenced Reboot*.
Sequence Reboot...	Opens the **Sequenced Reboot** window to execute a sequenced reboot. For more information, refer to Chapter 18, *Sequenced Reboot*.

Config Submenu

The **Config** submenu provides options that let you save, download, and compare configuration files. Table F-3 lists and describes the options in this menu.

Table F-3 Config Submenu Options

Option	Description
Save Baseline...	Opens the **Save Baseline -- Configuration Template Selection** dialog box so you can begin to save the configuration file of a switch to a server. For more information about how to save a baseline, refer to *Save a Baseline Configuration to a File* on page 16-3.
Compare/Download From File	Opens the **Compare/Download from File -- Select Baseline Configuration** window to choose a file to compare or download. For more information on comparing and downloading configurations, refer to Chapter 16, *Comparing Configurations*.
Compare/Download From Switch	Opens the **Compare/Download from Switch -- Source Configuration Selection** window to select a switch so you can compare to the configuration of that switch or download the configuration of that switch. For more information on comparing and downloading configurations, refer to Chapter 16, *Comparing Configurations*.

Licensing Submenu

The **Licensing** submenu provides options that let you manage licenses with Fabric Manager. Table F-4 lists and describes the options in this menu.

Table F-4 Licensing Submenu Options

Option	Description
Import from File...	Opens the **Import License -- Select license file** dialog box to import license keys from a file that you can apply to one or more switches. For more information on how to import a license file, refer to *Import and Export License Keys* on page 7-2.
Load from Switch...	Opens the **License Admin -- Switch Selection** window. For more information on how to load licenses from a switch, refer to Chapter 7, *Licensing*.
Generate Licenses...	Opens the **Create License Request -- Select transaction key file or saved request** window to obtain licenses and later apply them to switches.
Load Generated Licenses...	Opens the **License Admin -- Switch Selection** window to open previously saved license files, which you can then download to switches.

G

Help Menu Reference

This appendix contains the following sections

Introduction

The **Help** menu provides access to information about Fabric Manager. Table G-1 lists and describes the options that appear in the **Help** menu.

Table G-1 **Help Menu Options**

Option	Description
Help...	Opens **Fabric Manager Help**.
Context Help...	Creates a pointer to provide help about any portion of Fabric Manager that you click.
Status Legend...	Displays the Fabric Manager status legend.
About...	Provides information about your version of Fabric Manager.
Register...	Opens the **Fabric Manager Registration** dialog box. For details, refer to *Registering Fabric Manager* on page 2-14.

H

Zoning Reference

This appendix contains the following sections:

Introduction

This Appendix provides information about zoning fields. Table H-1 lists and describes the components of the **Zone Administration** window.

Zoning interfaces vary by firmware. Your interface may appear differently.

Table H-1 **Zone Administration Window Components**

Component	Description
File menu	Provides administrative options. For more information on the items in this menu, refer to *File Menu* on page H-3.
Edit menu	Lets you add, delete, replace, and search for zone member identifiers. For more information, refer to *Edit Menu* on page H-4.
View menu	Lets you choose a zoning display. For more information, refer to *View Menu* on page H-5.
Actions menu	Lets you enable, disable, and save zoning configurations. For more information, refer to *Actions Menu* on page H-6.
zoning type display	Appears beneath the **File** menu and displays the zoning type that you chose from the **View** menu.
Enabled Config display	Displays the enabled zoning configuration.
zoning configuration tabs	Let you configure zoning. For more information, refer to the tab-specific sections that follow: ◆ *The options available in the Action Menu of the Zone Administration window are described in Table H-5.* on page H-6 ◆ *Zone Tab* on page H-9 ◆ *QuickLoop Tab* on page H-11 ◆ *Fabric Assist Tab* on page H-13 ◆ *Config Tab* on page H-16

File Menu

Table H-2 describes the options that appear in the **File** menu of the **Zone Administration** window.

Table H-2 File Menu Options

Option	Description
Print Summary	Prints a zoning configuration report. A window displays both the effective configuration and the defined zoning configuration, if one exists.
Close	Closes the **Zone Administration** window.

Edit Menu

Table H-3 describes the options that appear in the **Edit** menu of the **Zone Administration** window.

Table H-3 Edit Menu Options

Option	Description
Add WWN...	Adds a WWN across aliases, zones, or Fabric Assist zones. A dialog box appears; enter the WWN number.
Delete WWN...	Deletes a WWN across aliases, zones, or Fabric Assist zones. A dialog box appears; enter the WWN number.
Replace WWN...	Replaces one WWN with another. A dialog box appears; enter first the WWN number to be replaced, and then the new WWN number.
Search Member...	Searches for a member of a zone. A dialog box appears; enter any element that appears in the **Member Selection List**: Domain Name, Port Name, Port ID, WWN, Device, Zone Name, or Alias Name. Narrow searches by selecting one or more of the following boxes: ◆ **Match Case** ◆ **Match whole words only** ◆ **Wrap around** Select the **Wrap around** box if you want the search engine to restart after it hits the end of the string. Leave cleared if you want the search engine to stop once it hits the end of the string; a message appears to indicate the search is complete.

View Menu

The options available in the **View** menu of the **Zone Administration** window are described in Table H-4.

Table H-4 View Menu Options

Option	Description
Mixed Zoning	Lets you include various objects as member of an alias, zone, or configuration file.
Port Zoning	Lets you include only ports in a group. Grouping zones by port alone constitutes "hard zoning".
WWN Zoning	Groups zones by World Wide Names. Grouping zones by WWN alone constitutes "hard zoning".
AL_PA Zoning	Lets you create or manage a zone of devices.
Refresh Zoning	Refreshes the zoning database. This will overwrite any unsaved zoning database changes you have made.
Refresh Fabric	Displays the latest fabric changes.

Actions Menu

The options available in the **Action Menu** of the **Zone Administration** window are described in Table H-5.

Table H-5 **Actions Menu Options**

Menu Item	Description
Enable Config	Saves and enables the configuration selected from the **Config** tab **Name** field. This command also saves all other configurations in the zoning database.
Disable Zoning	Disables the configuration that is currently enabled. A dialog box provides a warning before disabling.
Save Config Only	Saves all defined zoning configurations. The saved changes will only apply to the defined configurations. Changes can be made to a configuration that is currently enabled; changes will not appear until the configuration is disabled and reenabled.
Clear All	Deletes all aliases, zones, Fabric Assist zones, and configurations; the cleared configuration is saved. Any enabled configuration will be disabled.

Use the **Alias** tab to create, modify, rename, or delete aliases in the zoning database. An example of the **Alias** tab is displayed in Figure H-1.

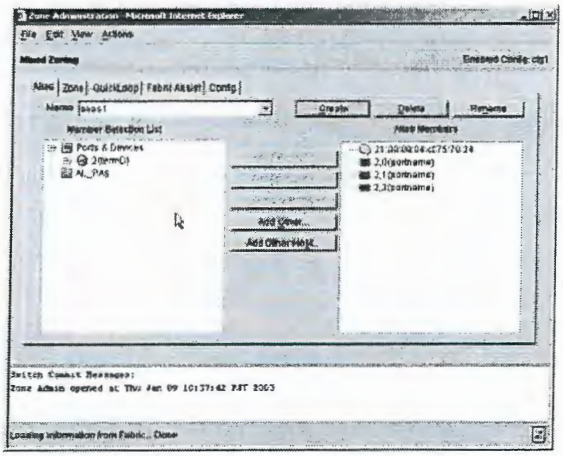


Figure H-1 **Alias Tab in the Zone Administration Window**

Alias Tab Descriptions

Table H-6 lists and describes the components of the **Alias** tab.

Table H-6 **Alias Tab Component Descriptions**

Component	Description
Name pull-down menu	Displays existing alias names from the pull-down menu.
Create button	Creates a new alias. A dialog box appears. Enter the name of the new alias. All names must be unique and contain no spaces.
Delete button	Deletes the alias selected in the **Name** field. Deleting an alias automatically removes it from all zones, and configurations.
Rename button	Renames the alias selected in the **Name** field. A dialog box displays in which you can rename the alias. Renaming an alias automatically renames it in all zones and configurations.
Member Selection List field	Selects available items from the **Member Selection List**. In Mixed zones you can select ports, WWNs, and AL_PAs.
Alias Members field	Displays the current members of an alias.

Table H-6 Alias Tab Component Descriptions (continued)

Component	Description
Add FA Host button	Adds a Fabric Assist host to the member list.
Add Member button	Adds a member from the **Member Selection List** to the **Alias Members** field. You must select a member within **Member Selection List** for this button to become active.
Remove Member button	Removes a member from the **Alias Members** list. You must select a member within **Alias Members** for this button to become active.
Add Other button ◆ Other ◆ Other Port ◆ Other WWN ◆ Other AL_PA	Adds a port, WWN or AL_PA that is not currently part of the fabric. A dialog box will appear for you to type in the host that is not a member of the fabric.
Add Other Host button ◆ Other Host ◆ Other Port Host ◆ Other WWN Host	Adds a host that is not currently part of the fabric. The button displayed depends on the zoning method that you have selected.

Zone Tab

Use the **Zone** tab to create, modify, rename, or delete zones in the zoning database. An example of a **Zone** tab is displayed in Figure H-2.

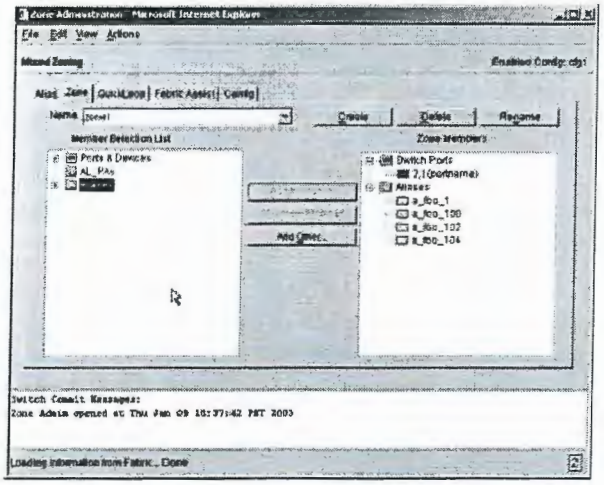


Figure H-2 **Zone Tab in the Zone Administration Window**

Zone Tab Descriptions

Table H-7 lists and describes the components of the **Zone** tab.

Table H-7 **Zone Tab Component Descriptions**

Component	Descriptions
Name pull-down menu	Displays existing zones from the pull-down menu.
Create button	Creates a new zone. A dialog box appears. Enter the name of the new zone. All zone names must be unique and must consist of letters, numbers, or the underscore character. Spaces or special characters are not allowed in zone names, and a name cannot start with a number.
Delete button	Deletes the zone selected in the **Name** field. Deleting a zone automatically removes it from all configurations.

Table H-7 Zone Tab Component Descriptions (continued)

Component	Descriptions
Rename button	Renames the zone selected in the **Name** field. A dialog box appears in which you can edit the zone name. Renaming a zone in the **Zone** tab automatically renames it in all configurations.
Member Selection List field	Lets you select available items from the **Member Selection List**.
Zone Members field	Displays the current members of a zone.
Add Member button	Adds a member from the **Member Selection List** to the **Zone Members** field. You must select a member within **Member Selection List** for this button to become active.
Remove Member button	Removes a member from the **Zone Members** field. You must select a member within the **Members Selection List** for this button to become active.
Add Other ◆ Other Port ◆ Other WWN ◆ Other AL_PA	Adds a port, WWN or AL_PA that is not currently part of the fabric. A dialog box will display for you to type in the host that is not a member of the fabric.

QuickLoop Tab

Use the **QuickLoop** tab to manage QuickLoops in the zoning database. For more information regarding QuickLoops, refer to your firmware documentation. An example of the **QuickLoop** tab is displayed in Figure H-3.

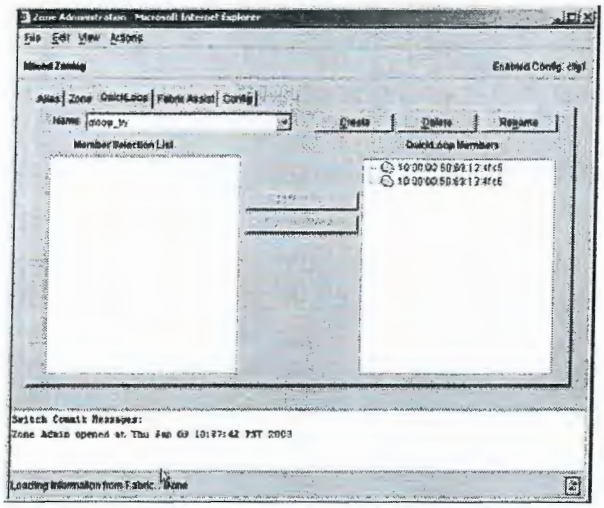


Figure H-3 **QuickLoop Tab in the Zone Administration Window**

QuickLoop Tab Descriptions

Table H-8 lists and describes the components of the **QuickLoop** tab.

Table H-8 **QuickLoop Tab Component Descriptions**

Component	Description
Name pulldown menu	Displays existing QuickLoops.
Create button	Creates a new QuickLoop. A dialog box appears. Enter the name of the new QuickLoop. All names must be unique and contain no spaces.
Delete button	Deletes the QuickLoop selected in the **Name** pull-down menu. Deleting a QuickLoop automatically removes it from all configurations.

Table H-8 QuickLoop Tab Component Descriptions (continued)

Component	Description
Rename button	Rename the QuickLoop selected in the **Name** pull-down menu. A dialog box appears in which you can edit the QuickLoop name. Renaming a QuickLoop automatically renames it in all configurations.
Member Selection List field	Lets you select available members from the **Member Selection List**. QuickLoop is not supported on switches that run firmware versions 4.x. However you can manage a QuickLoop from these switches if it is attached to another switch in the fabric.
QuickLoop Members field	Displays the current members of a QuickLoop.
Add Member button	Adds a member from the **Member Selection List** to the **QuickLoop Members** field. You must select a member within **Member Selection List** for this button to become active.
Remove Member button	Removes a member from the **QuickLoop Members** field. You must select a member within **QuickLoop Members** field for this button to become active.

Fabric Assist Tab

Use the **Fabric Assist** tab to create and manage Fabric Assist zones. Fabric Assist allows private hosts to communicate with public targets across a switched fabric. Fabric Assist also allows private hosts to communicate with public targets that do not reside in the same switched fabric.

You cannot create a fabric zone without a fabric host.

You cannot access the **Fabric Assist** tab if you selected **View > AL_PA Zoning**.

An example of a **Fabric Assist** tab is displayed in Figure H-4.

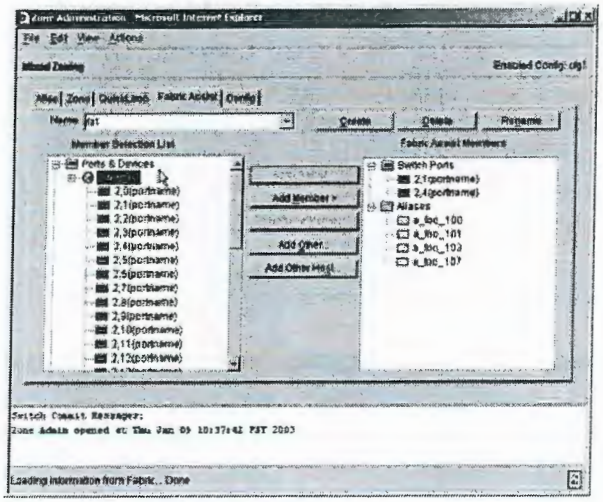


Figure H-4 **Fabric Assist Tab in the Zone Administration Window**

Fabric Assist Descriptions

Table H-9 lists and describes the components of the **Fabric Assist** tab.

Table H-9 Fabric Assist Components Descriptions

Components	Descriptions
Name pull-down menu	Displays existing Fabric Assist zones from the pull-down menu.
Create button	Creates a new Fabric Assist zone. A dialog box appears; Enter the name of the new Fabric Assist zone. All names must be unique and contain no spaces.
Delete button	Deletes the Fabric Assist zone selected in the **Name** pull-down menu. Deleting a Fabric Assist Zone automatically removes it from configurations.
Rename button	Renames the Fabric Assist zone selected in the **Name** pull-down menu. A dialog box appears in which you can edit the Fabric Assist name. Renaming a Fabric Assist Zone automatically renames it in all configurations.
Member Selection List field	Lets you select available items from the **Member Selection List**.
Fabric Assist Members field	Displays the current members of an Fabric Assist zone.
Add FA Host button	Adds a Fabric Assist host that is not currently part of the fabric.
Add Member button	Adds a member from the **Member Selection List** to the **Fabric Assist Members** field. You must select a member within **Member Selection List** for this button to become active.

Table H-9 Fabric Assist Components Descriptions (continued)

Components	Descriptions
Remove Member button	Removes a member from the Fabric Assist Members list. You must select a member within **Fabric Assist Members** field for this button to become active.
Add Other button ◆ Other ◆ Other Port ◆ Other WWN ◆ Other AL_PA	Adds a Fabric Assist zone that is not currently part of the fabric. A dialog box will appear for you to type in the host that is not a member of the fabric.
Add Other Host button ◆ Other Host ◆ Other Port Host ◆ Other WWN Host	Adds a host that is not currently part of the fabric. The button displayed depends on the zoning method that you have selected.

Config Tab

Use the **Config** tab to create and manage configurations. An example of the **Config** tab is displayed in Figure H-5.

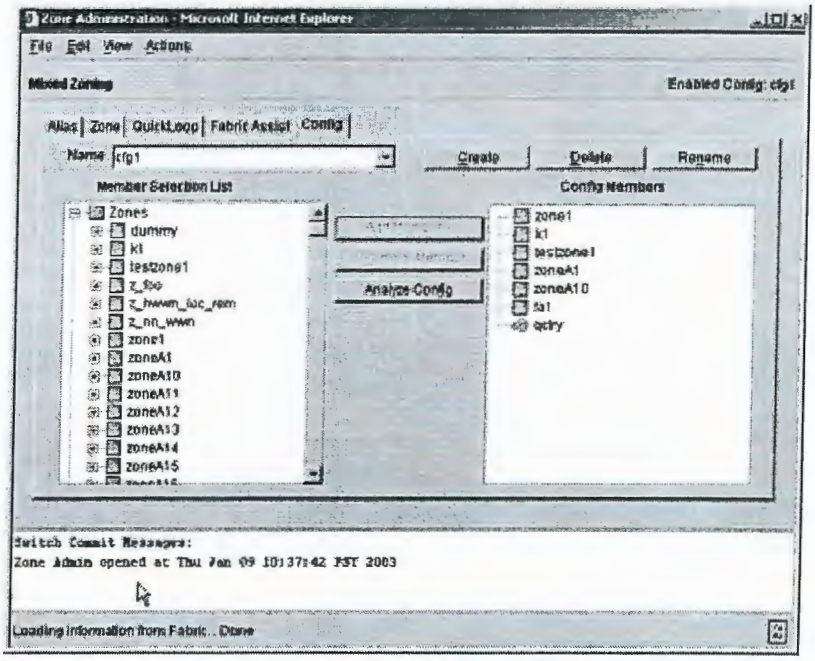


Figure H-5 Config Tab in the Zone Administration Window

Config Tab Descriptions

Table H-10 lists and describes the components of the **Config** tab.

Table H-10 Config Tab Component Descriptions

Component	Description
Name pull-down menu	Lets you select an existing configuration from the pull-down menu to display or modify.
Create button	Creates a new configuration. A dialog box appears; enter the name of the new configuration. All names must be unique and contain no spaces.
Delete button	Deletes the configuration selected in the Name pull-down menu. Deleting a configuration does not delete any of the elements contained in that configuration.
Rename button	Renames the configuration selected in the **Name** pull-down menu. A dialog box appears in which you can edit the configuration name.
Member Selection List field	Lets you select available items from the **Member Selection List**.
Config Members field	Displays the current config members.
Add Member button	Adds a member from the **Member Selection List** to the **Config Members** field. You must select a member within **Member Selection List** for this button to become active.
Remove Member button	Removes a member from the **Config Members List**. You must select a member within **Config Members** field for this button to become active.
Analyze Config button	Analyzes the configuration that is selected along with its member zones. A report is created that lists: ◆ SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration. ◆ SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration but not in the fabric.

I

Fabric Watch Reference

This appendix contains the following sections:

Introduction

The **Fabric Watch** window provides the fields you need to view and configure threshold and alarm settings. Table I-1 lists and describes the components of the window.

Table I-1 Fabric Watch Window Components

Component	Description
Fabric Watch navigation tree	Displays the various Fabric Watch classes that you can configure. For more information on how to configure Fabric Watch, refer to *How to Use Fabric Watch* on page 9-4.
Alarm Notification tab	Displays Fabric Watch alarms that fabric events have triggered. For more information, refer to *Alarm Notification Tab* on page I-3.
Threshold Configuration tab	Lets you configure threshold boundaries, traits, and alarms. For more information, refer to *Threshold Configuration Tab* on page I-4.
Email Configuration tab	Lets you configure the Fabric Watch e-mail alert alarm. For more information, refer to *E-Mail Configuration Tab* on page I-7

Alarm Notification Tab

Use the **Alarm Notification** tab of the **Fabric Watch** window to view the information for all Fabric Watch elements and classes. The **Alarm Notification** tab polls current events from Fabric Watch and refreshes the display according to the threshold configuration. Table I-2 lists and describes the components of the **Alarm Notifications** tab.

Table I-2 **Alarm Notification Tab Component Descriptions**

Component	Description
Selected Area pull-down menu	Displays the configurable areas in the pull-down menu. The items listed will change depending on the item selected in the navigation tree.
Name column	Displays the name of the alarm. Threshold names consist of the following three parts, with no separators: ◆ Class name abbreviation ◆ Area name abbreviation ◆ Element index number
State column	Displays the severity of the alarm that governs the kind of traps Fabric Watch employs in response to an event. The state of the alarm can be Informative, Normal, or Faulty.
Reason column	Displays the reason that an alarm notification was sent, such as Started, Changed, Exceeded, Below, Above, or In between.
Last Value column	Displays the value of a counter (behavior variable) prior to the alarm.
Current Value column	Displays the value of the counter (behavior variable) that set off the alarms.
Time column	Displays the time and date the notification was sent from the switch.

Threshold Configuration Tab

Use the **Threshold Configuration** tab to view and configure Fabric Watch thresholds for the Fabric Watch class that you select in the Fabric Watch navigation tree. Table I-3 lists and describes the components of the **Threshold Configuration** tab.

Table I-3 Threshold Configuration Tab Components

Component	Description
Select Area pulldown menu	Lists the areas of thresholds that you can configure. The areas that appear in the pulldown menu depend on the class that you select from the **Fabric Watch** navigation tree.
Area Configuration tab	Provides fields to configure Fabric Watch threshold boundaries and alarms. For more information, refer to *Area Configuration Tab* on page I-4.
Element Configuration tab	Provides fields to configure Fabric Watch threshold traits. For more information, refer to *Element Configuration Tab* on page I-5.
Configuration Report tab	Displays the Fabric Watch settings for the class that you select from the **Fabric Watch** navigation tree. For more information, refer to *Configuration Report Tab* on page I-6.

Area Configuration Tab

Table I-4 lists and describes the components of the **Area Configuration** tab.

Table I-4 Area Configuration Components

Component	Description
Boundary Partition	
Unit field	Sets or displays the selected unit values used for the chosen area. Depending on the area of interest, this is figured in units of *downs*, *reconfigs*, *errors*, *changes*, *logins*, etc.
High field	Sets or displays the number of high boundaries (the highest limit at which an element will not trigger an event) for the selected area.
BufferSize field	Sets or displays the threshold boundary buffer size of the selected area.

Table I-4 Area Configuration Components (continued)

Component	Description
TimeBase pull-down menu	Sets or displays the basic unit of time in which events are recorded for the selected area. The units available from the pull-down menu are: none, second, minute, hour, or day.
Low field	Sets or displays the number of low boundaries (the lowest limit at which an element will not trigger an event) for the selected area.
Select Boundary Level pull-down menu	Lets you select either a default or custom setting for the boundary levels. The default values are shown in parenthesis.
Alarm Setting Partition	
Alarm Notification Mechanisms checkboxes	Lets you select Alarm settings for Errorlog, SNMP, RAN, Portlog, and e-mail to be active on the switch side.
Select Alarm Level pull-down menu	Select either a custom or default setting for the alarm level; this setting will be active on the switch side menu.

Element Configuration Tab

Table I-5 lists and describes the components of the **Element Configuration** tab.

Table I-5 Element Configuration Tab Components

Component	Description
Select Element pulldown menu	Lets you choose a specific element to configure.
Status Partition	
Enable radio button	Enables alarms when selected.
Disable radio button	Disables alarms when selected.
Behavior Type Partition	
Triggered behavior radio button	Causes Fabric Watch to register an event when a variable exceeds a threshold. An event will not be triggered again until the variable falls and exceeds the threshold again.

Table I-5 Element Configuration Tab Components (continued)

Component	Description
Continuous radio button	Causes Fabric Watch to register an event when a variable exceeds a threshold and continue to register an event for every time interval.
Time Interval Partition	
Time Interval (in secs) pulldown menu	Lets you select the amount of time (in seconds) that you want Fabric Watch to poll for a new event.

Configuration Report Tab

Table I-6 describes the contents of the **Configuration Report** tab.

Table I-6 Threshold Configuration Report Component Descriptions

Component	Description
Configuration for Class	Describes the class that is being reported. The item selected in the Navigation tree appears here.
Begin Area	Describes the current settings configured for the selected area. Refer to <Link>Table I-5.
Begin Element	Describes the current settings configured for the selected area.
Changed	Displays thresholds that have changed.
Exceeded	Displays thresholds that have been exceeded.
Below	Displays thresholds that have fallen below the configured level.
Above	Displays thresholds that have risen above the configured levels.
In Between	Displays thresholds that have are in within the configured level.

E-Mail Configuration Tab

Use the **E-mail Configuration** tab to enable and configure e-mail alarm notifications. A different e-mail configuration can be set for each Fabric Watch class. For example, one e-mail notification can be set for SFPs and another can be set for E-Ports (see the navigation tree).

The Fabric Watch **E-mail Configuration** components are described in Table I-7.

Table I-7 **Email Configuration Component Descriptions**

Component	Description
Mail To: field	Accepts the e-mail address that Fabric Watch e-mails when an event occurs that triggers an e-mail alert.
Mail Status partition	Lets you enable or disable email alert.
Mail Validation partition	Gives you the option to send a test e-mail to the recipient in the **Mail To:** field when you click **Apply**.
Apply button	Applies your configuration.
Reset button	Resets the fields to default values.

J

CallHome External Executable Reference

This appendix contains the following sections:

Introduction

The Call Home feature of Fabric Manager can accept an external executable that runs when a Call Home event occurs. If you configure an external executable, Fabric Manager passes an XML file to the executable when the event occurs. All other functionality is at your discretion.

Large executables may impair the performance of your server.

Call Home Executable Requirements

- The executable must run on a Windows platform. You can use any type of executable as long as it is a valid executable for Windows.
- The executable must be able to handle Fabric Manager passing it a command-line argument. The argument is the name of an XML file that Call Home generates when an event occurs.

Example

If I enter the executable `C:\executable.exe` in the **External Executable on Server** field in my Call Home window, Call Home launches `C:\executable.exe` *`filename`*`.xml` when an event occurs.

Any additional executable requirements depend on your needs.

K

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure K-1).

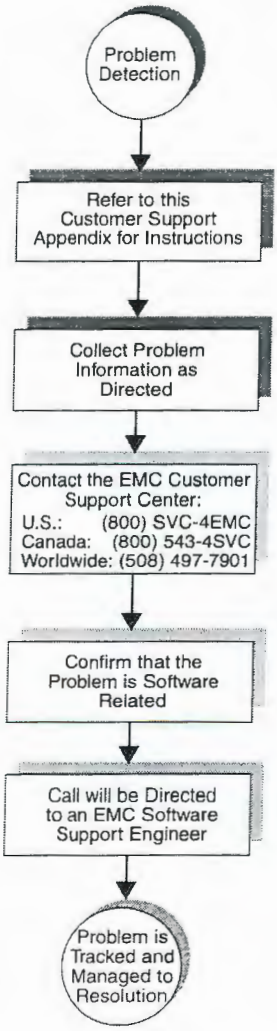


Figure K-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.EMC.com`

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- E-mail
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 Fibre Channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Security feature that enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated Loop Physical Address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. Tee 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from overheating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection-oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the runtime operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel The left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides Ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

Device Connection Controls Feature that enables organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by a WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to departmental switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense Wavelength Multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error Detect Time-Out Value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-End credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control A means to govern the flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest-level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

Fabric Access A means to allow 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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s Gigabytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode*.

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit*.

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL*.

M

Media See *Transceiver*.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port*.

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign domain IDs. The role of principle switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource Allocation Time-Out Value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15 to 25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A Brocade product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the departmental switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-Level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-Level Time-Out Value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

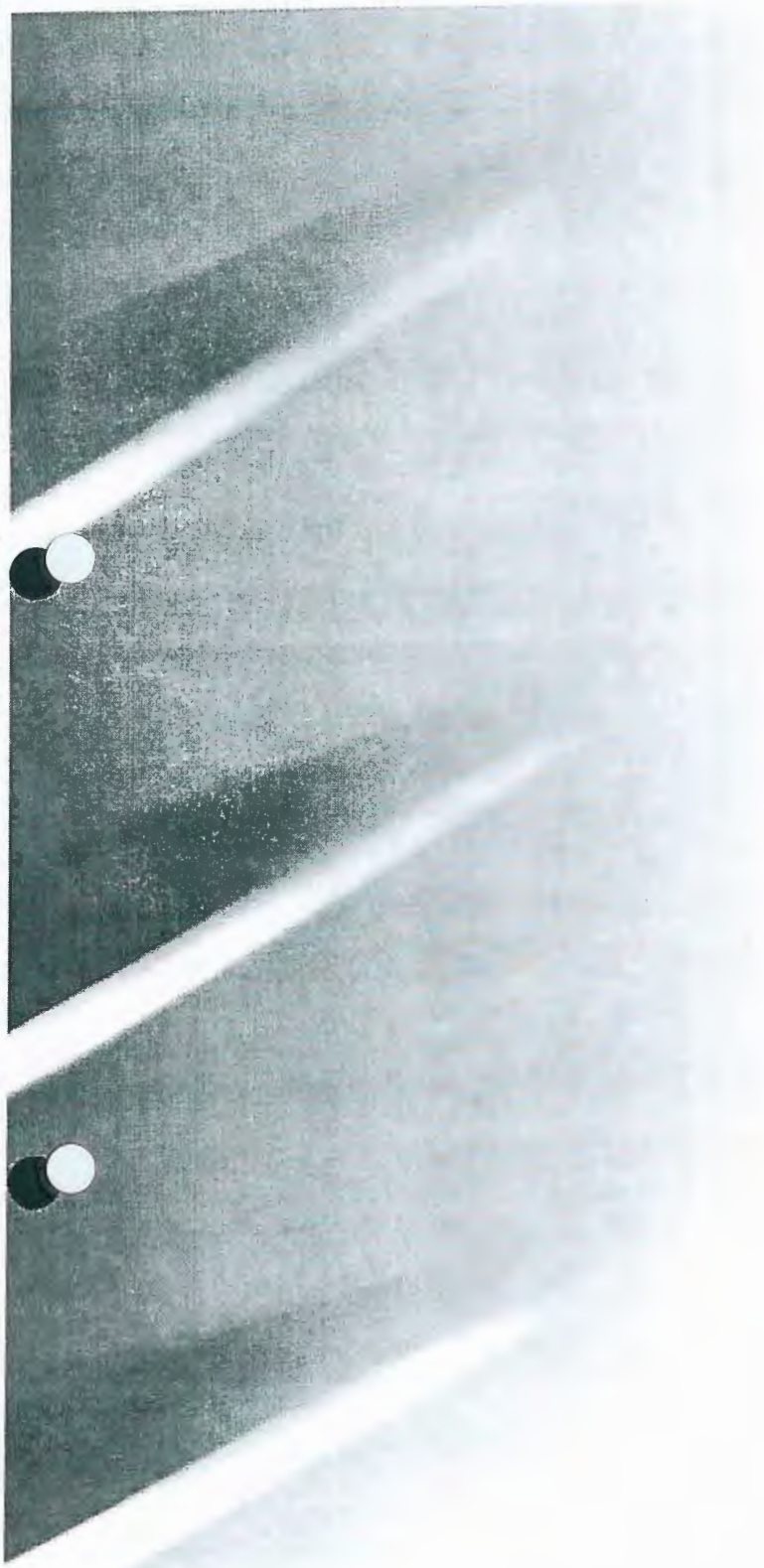
Index

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

22143

ANEXO SWITCH TIPO 03
PARTE 5

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br



EMC Connectrix B Series
Fabric Watch
Version 3.1 and Version 4.1

REFERENCE MANUAL

P/N 300-000-643
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

Connectrix B Series systems have been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Preface

The EMC Connectrix B Series EMC Connectrix B Series Fabric Watch Reference Manual provides information on Fabric Watch that you may encounter during installation and operation of the DS-16B2, DS-32B2, and ED-12000B.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch and Enterprise Director. For the most up-to-date information on product features, see your product release notes.

If a feature in the DS-16B2, DS-32B2, or ED-12000B does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

This guide is part of the EMC Connectrix DS-16B2, DS-32B2 and ED-12000B documentation set, and is intended for use by system administrator during installation and configuration of the DS-16B2, DS-32B2 and ED-12000B switches.

Readers of this guide are expected to be familiar with the EMC Connectrix DS-16B2, DS-32B2 and ED-12000B operating environment.

Organization

This manual provides the following information about Fabric Watch:

Chapter 1, *Introducing Fabric Watch*, describes the features and functions of EMC Connectrix DS-16B2, DS-32B2 and ED-12000B Fabric Watch.

Chapter 2, *Installing Fabric Watch*, provides information for installing Fabric Watch.

Chapter 3, *Using Fabric Watch*, describes methods for using Fabric Watch.

Appendix A, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix DS-16B2, DS-32B2 and ED-12000B.

The *Glossary* provides explanations for terminology used in this manual.

Related Documentation

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-16B2 QuickLoop Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*

- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this guide:

Palatino, bold	◆ Dialog box, button, icon, and menu items in text ◆ Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
Courier, italic	Arguments used in examples of command line syntax.

Courier	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

Courier, bold	◆ User entry. For example: **`symmpoll -p`** ◆ Options in command line syntax
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.EMC.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

```
http://powerlink.EMC.com
```

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to `techpub_comments@EMC.com` with your opinions of this guide.

1 Introducing Fabric Watch

Fabric Watch is an optionally licensed product. This chapter provides the following information:

Overview

Fabric Watch software monitors the performance and status of switches, and can alert storage area network managers when problems arise. The real-time alerts from Fabric Watch software help SAN managers solve problems before they become costly failures. SAN managers can configure Fabric Watch software to monitor any of the following:

- Fabric events (such as topology reconfigurations and zone changes)
- Physical switch conditions (such as fans, power supplies, and temperature)
- Port behavior (such as state changes, errors, and performance)
- Small form factor pluggable (SFP) (for switches equipped with SMART SFPs)

With Fabric Watch software, SAN managers can place limits, or *thresholds*, on the behavior of different switch and fabric elements. Fabric Watch then monitors these behavior variables, or *counters*, and issues an alarm when a counter crosses a threshold. An alarm may email the SAN manager or forward all error information to a proxy switch; the response depends upon how the manager configures the alarm.

Elements and Components

Fabric Watch software uses a number of terms and components to identify, classify, monitor, and handle fabric and switch activity.

Element Categories

Fabric Watch elements include any component of the fabric or switch that Fabric Watch software monitors. To monitor elements, Fabric Watch software categorizes them into *areas*, and groups areas into *classes*.

Classes

Classes (also known as *agents*) are high-level categories of elements. Fabric Watch software monitors elements that compose the following classes:

- Fabric
- Environment
- Port (includes E_Port, Optical F/FL_Port, and in 3.0 only; Copper F/FL_Port)
- SFP
- Performance Monitor (Alpa, End-to-End, Filter)

Areas

Areas are the behaviors that Fabric Watch software monitors. Table 1-1 lists all Fabric Watch classes, the areas within those classes, and a description of each area.

Table 1-1 Fabric Watch Areas

Class	Area	Area Description
Fabric	E_Port down	Monitors E_Port status.
	Fabric reconfiguration	Monitors changes to the fabric configuration.
	Segmentation changes	Monitors segmentation changes.
	Domain ID changes	Monitors forcible Domain ID changes.
	Zoning changes	Monitors changes to currently enabled zoning configurations.
	Fabric logins	Monitors the number of host device fabric logins (FLOGI).
	SFP changes	Monitors insertion/removal of smart SFP.
Environmental	Temperature	Monitors switch temperature in degrees Celsius.
	Fan	Monitors switch fan speed in rpms.
	Power supply	Monitors whether the power supply is functional or faulty.

Table 1-1 Fabric Watch Areas *(continued)*

Class	Area	Area Description
Port	Link failure count (link loss)	Monitors the link failure rate of each port. Tracks the number of link failures per configured time interval.
	Loss of synchronization count	Monitors the number of synchronization loss errors per configured time interval.
	Loss of signal count	Monitors the number of signal loss errors per configured time interval.
	Primitive sequence protocol error	Monitors the number of protocol errors per configured time interval.
	Invalid transmission word	Monitors the number of invalid words transmitted (from a device to a port) per configured time interval.
	Invalid CRC count	Monitors the number of CRC errors per configured time interval.
	Receive performance	Monitors receive rate in KB/s.
	Transmit performance	Monitors transmit rate in KB/s.
	State changes	Monitors state changes.
SFP	Temperature	Monitors SFP temperature in degrees Celsius.
	Receiver power	Monitors SFP receiver power in uwatts.
	Transmitter power	Monitors SFP transmitter power in uwatts.
	Current	Monitors SFP current in mamps.

Table 1-1 **Fabric Watch Areas *(continued)***

Class	Area	Area Description
Performance Monitor	Invalid CRCS	Monitors the number of CRC errors that occur (for ALPA or for a SiD-DiD pair) per configured time interval (in seconds).
	RX Performance	Monitors receive rate of a SiD-DiD pair in KB/s.
	TX Performance	Monitors transmit rate of a SiD-DiD pair in KB/s.
	Customer Define	Monitors the filter-based counter that the user defines.
FRU	Slot	Monitors slot status.
	Power Supply	Monitors power supply status.
	Fan	Monitors fan status.
	WWN	Monitors WWN status.

Monitoring Tools

Fabric Watch uses a number of tools to:

- Monitor switch performance
- Monitor fabric performance
- Alert SAN managers to potential problems

Counters

Counters represent the value of a behavior variable. Counters can be cumulative or current. For instance, a counter may represent the total number of times that a given error occurred since Fabric Watch began logging occurrences of that error, or it may represent the current speed in rpms of a fan. Fabric Watch compares counter values to threshold values to determine when events occur.

Thresholds

A threshold is a value or range of values to which Fabric Watch compares a behavior counter to determine if the behavior value is correct or warrants an alarm.

Range Threshold

A range threshold consists of a maximum and minimum boundary, and all values between the boundaries form a *normal* region. If a behavior counter exceeds (crosses) either boundary, that occurrence registers as an *event*. SAN managers can also configure Fabric Watch to register an event when a counter returns to a *normal* value.

Counters may oscillate around the upper or lower boundary of a range threshold, and as a result cause numerous events in a short period of time. To reduce the number of events, you can configure *buffers*, or ranges of values just below the upper boundary and just above the lower boundary. When a counter changes from a value that exceeds a threshold to a value that falls within the buffer zone, the counter does not register an event. An event will only register if the counter returns to a *normal* value beyond the buffer.

Figure 1-1 on page 1-8 illustrates a range threshold with buffers. The values at 1 second, 3 seconds, and 5 seconds generate events because they exceed boundaries. The value at 2 seconds does not generate an event because, though it crosses the boundary, it remains in the buffer zone. The values at 4 seconds and 6 seconds generate an event because they cross the upper boundary and lower boundary respectively, and return to a value beyond the buffer zone.

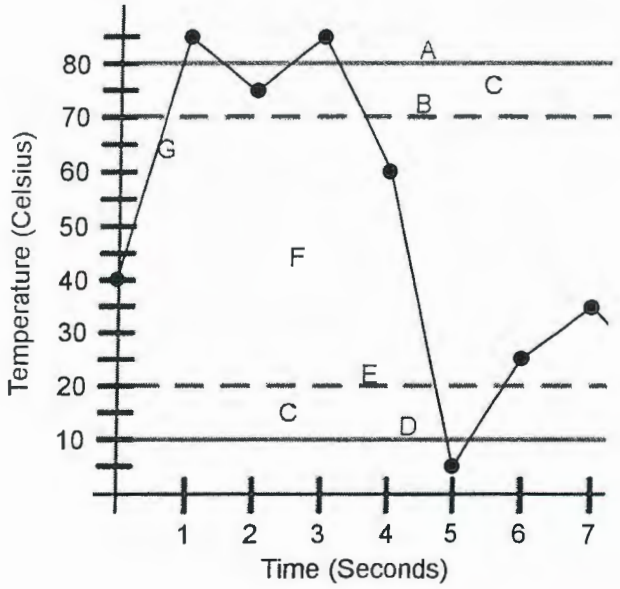


Figure 1-1 Range Threshold

Rising/Falling Threshold

A rising/falling threshold has only one boundary, not two like the range threshold. Where a range threshold has a *normal* state where a counter stays in between two boundaries, a rising/falling threshold is *normal* as long as the value of the counter does not exceed the value of the one boundary. Figure 1-2 on page 1-9 presents a rising/falling threshold. An event registers at 5 seconds when the counter value exceeds the boundary.

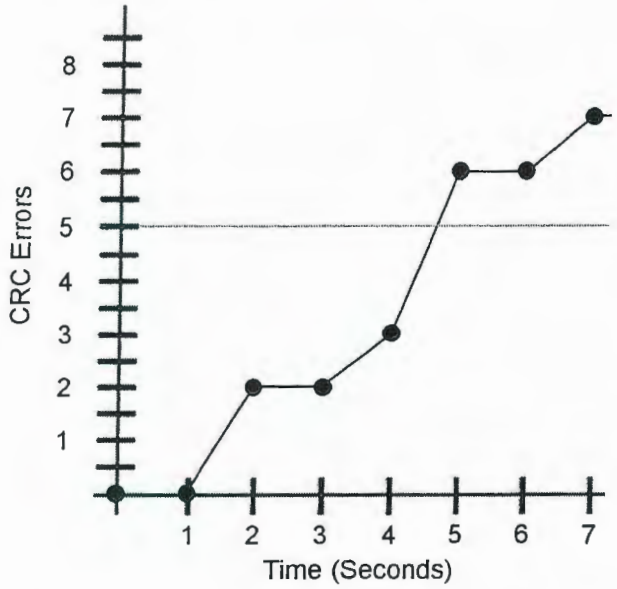


Figure 1-2 **Rising/Falling Threshold**

Change Monitor Threshold

A change monitor threshold consists of a number of distinct values, not a range of values. Whenever a behavior variable changes from one value to another, that change registers as an event.

Threshold Naming Conventions

You need to recognize threshold naming conventions so you can identify thresholds that appear in Fabric Watch error messages. All threshold names consist of the following three items, in the following order, with no separators:

1. Abbreviation of the threshold's class name, in lower case, refer to Table 1-2.

Table 1-2 **Class Name Abbreviations**

Class	Abbreviation
Fabric	fabric
Environment	env
Port	port
E_Port	eport

Table 1-2 Class Name Abbreviations (*continued*)

Class	Abbreviation
Optical F/FL_Port	fopport
Copper F/FL_Port	fcuport
SFP	sfp
Alpa Performance Monitor	alpa
End-to-End Performance Monitor	ee
Filter Performance Monitor	filter

2. Abbreviation for the area name is shown in Table 1-3.

Table 1-3 Area Name Abbreviations

Area	Abbreviation
Power supply	PS
Temperature (sensor)	Temp
Fan speed sensor	Fan
Receiver power	RXP
Transmitter power	TXP
Current	Crnt
Invalid CRCs	CRCs
Link failures	Link
Protocol errors	ProtoErr
RX Performance	RXPerf
Loss of Signal	Signal
State Changes	State
Loss of Sync	Sync
TX Performance	TXPerf
Invalid Words	Words
Domain ID	DI

Table 1-3 Area Name Abbreviations (*continued*)

Area	Abbreviation
E_Port down	ED
Fabric login	FL
Fabric reconfigure	FR
SFP state change	SS
Segmentation change	SC
Zoning change	ZC
Name server login	NL
Name server request	NR
Invalid CRCs	CRC
TX performance	TX
RX performance	RX
Filter frame counter	PT

3. Index number for the element involved.

   The index number consists of three digits and corresponds to where the element appears in respect to others in a series. For instance, if the element in question is the third temperature sensor on a switch, its number would be 003.

   Numbering for all port and SFP classes begin with index number 000 (as per the Fabric OS port numbering convention), but environment class index numbers begin with 001. Therefore, the first element in a series of ports will be 000, but the first element in a series of thermometers will be 001. For the fabric class, the index number is always 000. The threshold name is case sensitive.

Example `fopportState003` represents a state threshold of the fourth port (which contains an optical SFP).

Threshold Boundaries

Boundaries are the characteristics that define a threshold. Boundaries are area-based; when you configure a boundary, that boundary applies to every element in an area. Boundaries are non-volatile; you do not need to reconfigure your boundaries when you restart your switch. Table 1-4 lists the boundaries that can define a threshold and what each boundary identifies.

Table 1-4 **Threshold Boundaries**

Boundary	Definition
Unit string	Unit of measurement that Fabric Watch alarms will use to display the value of a particular counter. You can change the unit string to an arbitrary value with the `Fwconfigure` command.
Time base	Basic unit of time in which events are recorded.
Low boundary	Lowest limit at which the monitored value of an element will not register as an event.
High boundary	Highest limit at which the monitored valued of an element will not register as an event.
Buffer size	Size of a threshold buffer. The buffer size determines the distance between the upper buffer and the upper boundary, and the distance between the lower buffer and the lower boundary. The buffer size establishes the buffer zones, refer to Figure 1-1 on page 1-8.

Threshold Traits

You configure threshold traits to determine whether and when an event registers against a given threshold. Threshold traits determine the behavior of a threshold.

These traits are element-based, so you must configure traits for each individual element. Threshold traits are volatile, so you must reconfigure all traits after you restart your switch.

Table 1-5 lists and explains threshold traits.

Table 1-5 Threshold Traits

Trait	Definition
Status	Configures a threshold as enabled or disabled. Thresholds are enabled by default.
Behavior type	Configures a threshold as continuous or triggered. Thresholds are triggered by default.
Behavior interval	Configures the minimum time interval (in seconds) between two instances of the same type of alarm. The default interval is 1 second.

Behavior Types

The behavior type (or *mode*) of a variable determines the conditions under which Fabric Watch software registers an event. You can configure an area to respond to triggered or continuous behavior.

Triggered Behavior

In triggered behavior mode, Fabric Watch only registers an event when a variable exceeds a threshold. To trigger another event, the variable must cross the threshold again. For example, if the temperature of a switch exceeds its threshold while in triggered behavior mode, Fabric Watch only registers one event (such as an Above event or a Below event) until the temperature falls within the threshold, and then exceeds the threshold again.

Continuous Behavior

In continuous behavior mode, Fabric Watch registers an event when a variable exceeds a threshold and continues to register an event every designated time interval until the variable falls within the threshold again. SAN managers designate the time interval, or *behavior interval*.

Events

Whenever a counter exceeds a threshold, Fabric Watch software identifies that occurrence as an *event*. You can configure Fabric Watch so that events trigger alarms that notify you that the event took place.

Fabric Watch software recognizes six types of events. Table 1-6 describes Fabric Watch event types.

Table 1-6 Event Types

Event Type	Explanation	Associated Behavior Mode
Started	Element monitoring is in a started condition. A started event is not referenced. No alarms are available.	triggered/continuous
Below	A counter is below the lower boundary.	triggered/continuous
Above	A counter is above the upper boundary.	triggered/continuous
Exceeded	A counter is below the lower boundary or above the upper boundary.	triggered/continuous
Changed	A counter value has changed. A changed event is not referenced to any threshold boundary level. Changed events will be reported in reference to the behavioral interval time setting.	triggered/continuous
In-between	A counter falls below the upper boundary minus the buffer, or rises above the lower boundary plus the buffer. Must be preceded by an Above or Below event. If the buffer is set to zero, this event is suppressed.	triggered/continuous

Alarms

Fabric Watch software can notify SAN managers of events with a number of types of alarm.

Switch Event Log Entry

The switch event log holds up to 1536 entries. You can configure Fabric Watch software to forward event log entries to the SYSLOGD facility. This alarm stores event information for SAN managers, but does not actively alert SAN managers to events.

SNMP Trap

An SNMP trap forwards the following information to an SNMP management station:

- Name of the element involved in the event
- Class, area, and index of the threshold
- Type of event
- Value of the element that exceeded the threshold

- State of the element
- Source of the trap

This alarm stores event information for SAN managers, but does not actively alert SAN managers to events.

RapiTrap

EMC does not support this functionality.

RapiTrap actively alerts SAN managers to events. Once you enable RapiTrap, Fabric Watch forwards all event information to a designated proxy switch. (The host API automatically configures the proxy switch based on firmware version.) The switch then forwards the information to a server and alerts the SAN manager to event activity.

Email Alert

Email Alert sends information about a switch event to a specified email address. Email Alert can send information about any error from any element, area, and class. The email specifies the threshold and describes the event, much like an error message. You must use the `fwMailCfg` command to configure email alerts.

Severity States

Severity states appear in error messages to indicate the urgency of each alarm. Table 1-7 lists the various severity states. Only states 3 and 4 appear in user messages. All other states are MIB-related.

Table 1-7 Severity States

Severity Level	Traps
0	send no event traps
1	critical
2	error
3	warning
4	informational
5	debug

Configurations

SAN managers can use configuration files and Fabric Watch-specific configuration files, called *Profiles*, to customize Fabric Watch and store customized instructions.

Configuration File

The configuration file of a switch includes all Fabric Watch configuration information. You can edit a configuration file in a text editor to manually configure Fabric Watch thresholds and alarms. For more information, refer to *Edit the Configuration File* on page 3-8.

Fabric Watch Configurations

Fabric Watch configurations, also known as *Profiles*, are preset subsets of configuration files that cater to particular types of networks. You can download a Fabric Watch configuration to your switch and then configure Fabric Watch software to run from the subset or from your standard configuration file.

Fabric Watch configurations for switch management by SNMP can be accessed on the EMC website through the following steps:

1. Go to the Powerlink website:

   `http://www.powerlink.EMC.com`

2. Select **Services, Document Library, Connectrix**.
3. Scroll down to the desired files.

Default vs. Custom

Fabric Watch includes a default value for each element that you can configure. These default values constitute the default configuration. You cannot alter the default values. Fabric Watch maintains a second, custom configuration that you can customize. To use custom values, configure your custom values and set Fabric Watch to use the custom configuration.

If a default value matches a custom value, you can save memory if you enter no custom value at all and configure Fabric Watch to use the default value.

2 Installing Fabric Watch

This chapter provides the following information to describe two methods for installing Fabric Watch:

Overview

Fabric Watch software is optionally licensed software that resides on EMC switches, and that you can activate with the proper license. Contact an EMC Sales Representative to obtain a license key.

You can use Telnet commands or EMC Web Tools to install a Fabric Watch license.

Installing Through Telnet

To install Fabric Watch using Telnet commands:

1. Log on to the switch by Telnet (refer to the appropriate *EMC Connectrix Fabric OS Reference Manual* for details), using an account that has administrative privileges.
2. To determine whether a Fabric Watch license is already installed on the switch, type `licenseShow` on the Telnet command line.

   A list displays all the licenses currently installed on the switch.

   If the Fabric Watch license is not included in the list or is incorrect, continue with step 3.
3. Enter the following on the command line:

   ```
   licenseAdd key
   ```

   where `key` is the license key provided to you, surrounded by double quotes. The license key is case sensitive and must be entered exactly as given.
4. Verify the license was added by entering the following on the command line:

   ```
   licenseShow
   ```

   If the license is not listed, repeat step 3.

Installing Through Web Tools

To install Fabric Watch using Web Tools:

1. Launch the web browser, enter the switch name or IP address in the **Location/Address** field and press **ENTER**.

   http://111.222.33.1

   Web Tools launches, displaying the Fabric View.

2. Click the **Admin** button on the relevant switch panel.

   The logon window displays.

3. Enter a logon name, **admin** and password, **password** and press **ENTER**.

   The Administration View displays.

4. Click the **License Admin** tab, enter the license key in the **License Key** field, and click **Add License**.

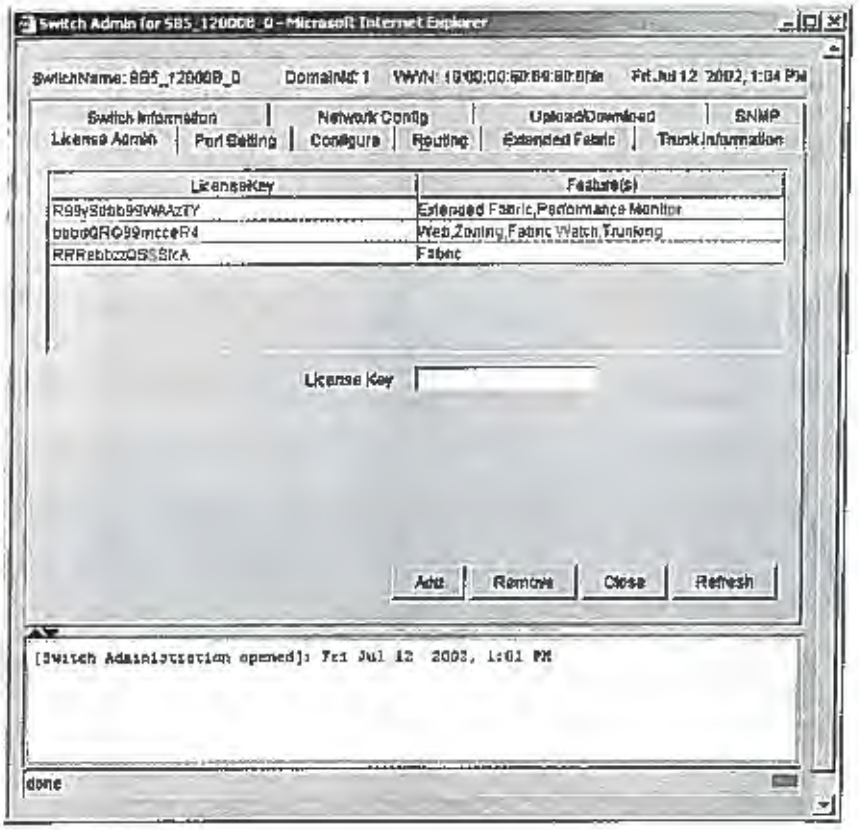


Figure 2-1 License Admin Tab

3 Using Fabric Watch

This chapter describes the procedure for using Fabric Watch and provides the following information:

Overview

You can use several user interfaces to configure Fabric Watch software. The sections that follow describe the various interfaces and explain how to configure various elements of Fabric Watch using the Telnet interface. For more information on Web Tools, refer to the appropriate *EMC Web Tools User Guide*.

User Interfaces

Use Web Tools, Telnet interface, an SNMP-based enterprise manager, or the configuration file to view and modify Fabric Watch settings.

Web Tools

Through Web Tools, you can:

- View fabric and switch events through the fabric wide Event View.
- View and modify threshold and alarm configurations through the Fabric Watch View.
- Upload and download the configuration file through the Config Admin tab in the Switch Admin window.

Refer to the *appropriate EMC Connectrix Web Tools User Guide* for information on using Web Tools.

Telnet Interface

You can use a Telnet interface to:

- Query fabric and switch events through the Telnet command `fwShow`.
- Query and modify threshold and alarm configurations. Use the the Telnet command `fwConfigure` to view the default and customized settings.
- Upload and download the configuration file through the commands `configUpload` and `configDownload`.

SNMP-Based Enterprise Managers

With SNMP-based enterprise managers you can:

- Query the MIB variable for individual fabric and switch elements.
- Query and modify threshold and alarm configurations.
- Receive generated SNMP traps when threshold conditions are met.

Configuration File

With Fabric Watch configurations, you can:

- Upload a configuration file.
- Make changes in a text editor.
- Download a file to all switches in a fabric to ensure a uniform configuration file throughout the fabric.
- Upload and download the configuration file through a Telnet session or with Web Tools.

How to Configure Fabric Watch With Telnet

When you install the license to activate Fabric Watch, the software runs based on default settings. You cannot alter the default settings; instead, you assign custom settings and configure Fabric Watch to use those settings. To use Fabric Watch, you must:

- Choose elements that you want to monitor.
- Place limits on the acceptable behavior of those elements (configure threshold boundaries).
- Choose the circumstances under which Fabric Watch identifies the behavior of an element as errant (configure behavior types).
- Turn Fabric Watch on (configure status).
- Choose if and how Fabric Watch alerts you to errant behavior (configure alarms).

The following sections discuss how to use Telnet commands to configure and use Fabric Watch software.

Configure Threshold Boundaries

Configure threshold boundaries to establish what behaviors will trigger events. (Remember, you can only change custom settings.)

To configure threshold boundaries, perform the following steps:

1. Open a Telnet session to your switch.
2. Enter the `fwConfigure` command. A list of Fabric Watch classes appears.
3. Select the class of the threshold that you want to configure. A list of the areas in that class appear.
4. Select the area of the threshold that you want to configure. A status display of that area and a list of configuration options appear.
5. Select **advanced configuration** to view configurable boundaries.
6. Select the boundary that you want to change. Fabric Watch presents a range of new values to choose from. (In the example below, options 4 through 8 represent the boundaries that you can configure.)
7. Enter the new boundary value.

8. Repeat step 6 until you have configured each boundary that you want to change.
9. Select **apply threshold boundary changes** to configure Fabric Watch to use the boundary settings that you customized. Remember, you cannot change default settings, you can only configure custom settings, then configure Fabric Watch to use those custom settings.

Configure Behavior Types With Threshold Traits

Configure behavior types to determine the circumstances under which an event registers and an alarm sounds. To configure behavior types with threshold traits, perform the following steps:

1. Run Fabric Watch and navigate to the advanced configuration menu (refer to *Configure Threshold Boundaries* on page 3-5).
2. Select **change behavior type**. Fabric Watch displays a range of threshold indexes.
3. Select the index number of the threshold that you want to configure.
4. Select a behavior type.

Configure Behavior Intervals With Threshold Traits

Configure behavior intervals to determine how frequently a continuous event registers. To configure behavior intervals with threshold traits, perform the following steps:

1. Run Fabric Watch and navigate to the advanced configuration menu.
2. Select **change behavior interval**.
3. Select the index number of the threshold that you want to configure. Fabric Watch presents a range of new values to choose from.
4. Enter a new behavior interval value.

Configure Status

Configure status to enable or disable thresholds. If you disable a threshold, Fabric Watch stops monitoring the related element. To configure status to enable or disable thresholds, perform the following steps:

1. Run Fabric Watch and navigate to the **select an area** menu (refer to *Configure Threshold Boundaries* on page 3-5).
2. Select an area. Fabric Watch displays a list of available thresholds.
3. Select **disable a threshold** or **enable a threshold**.
4. Select a threshold index. Fabric Watch enables or disables the threshold that you select.

Configure Alarms

Configure alarms to determine how Fabric Watch responds to each event.

When you configure alarms, you change the custom alarm configuration. Once you change the configuration, you must configure Fabric Watch to use the custom configuration.

To configure alarms, you must choose what alarms each event type will trigger. Fabric Watch uses a binary matrix to assign a numerical value to each alarm. To assign alarms to an event type, choose the alarms you want, add the numerical values of the alarms, and use the total value to map the alarms to the event. Table 3-1 lists the numerical values of each type of alarm.

Table 3-1 Alarm Values

Alarm	Matrix Value
None	0
Error Log Entry	1
SNMP Trap	2
RapiTrap	8
Email Alert	16

To configure alarms:

1. Run Fabric Watch and navigate to the advanced configuration menu (refer to *Configure Threshold Boundaries* on page 3-5).
2. Select the event type that will trigger the alarm(s) that you choose. In the following example, options 12 through 16 represent the different behaviors that can trigger an alarm.
3. Choose which alarms you want the event type to trigger, refer to Table 3-1. Locate the matrix values for each alarm. Add the matrix values and enter the sum at the Telnet prompt. For example, if you want an event to trigger a log entry (matrix value: 1)and an email alert (matrix value: 16), enter **17** at the prompt.
4. Select **apply threshold alarm changes** to configure Fabric Watch to use the alarm settings that you customized.

Edit the Configuration File

To edit the configuration file, upload the file to a host, then edit the file in a text editor and download the file to your switch.

To edit the configuration file, do the following:

1. Use the `configUpload` command to upload your configuration file to a host. Use the following command names and operands to upload the configuration file:

```
configUpload
   "<server>","<user-name","<filename>","<password>"
sw5:admin> configUpload
   "citadel","jdoe","config.txt","passwd"
upload complete
```

2. Edit the configuration file in a text editor.
3. Use `configDownload` to download your configuration file to your switch:

```
sw5:admin> configDownload
   "citadel","jdoe","config.txt"
Committing configuration...done.
download complete
```

4. Use `fwConfigReload` to load the new configuration:

```
sw5:admin> fwConfigReload
fwConfigReload: Fabric Watch configuration reloaded
```

Download a Fabric Watch Configuration

You can download available profiles from the following website:

`http://powerlink.emc.com`

How to Read Error Messages

To accurately read an error message, identify the following components of the message:

- Error identifier
- Date and time that the error occurred
- Type of event
- Threshold name
- Threshold label
- Element index number
- Element state

Example

```
0x10257b80 (tThad): Oct 25 09:52:21
   WARNING FW-BELOW, 3, sfpCrnt004 (Sfp Current 4) is
   below low boundary. current value : 0 (1 OK/0 FAULTY).
   (faulty)
```

Table 3-2 lists the components of this example message.

Table 3-2 Error Message Components

Component	Example
Error identifier	0x10257b80
Date and time	Oct 25 09:52:21
Type of event	WARNING FW-BELOW (a Below event)
Threshold name	sfpCrnt004
Threshold label	Sfp Current 4
Element index number	004
Element state	faulty

Threshold name in error messages = class name + area name + element index.

Example

```
class name = SFP,
area name = Cent,
element index = 004
threshold name is sfpCrnt004
```

For a complete list of class and area abbreviations, refer to Table 1-2 on page 1-9 and Table 1-3 on page 1-10.

A

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure A-1).

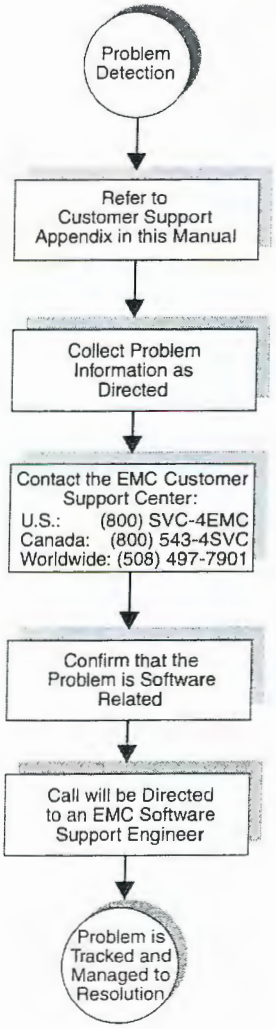


Figure A-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.EMC.com`

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding; LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. Tee 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-End credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In Order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode.*

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit.*

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL.*

M

Media See *Transceiver.*

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port.*

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A Brocade product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850nm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

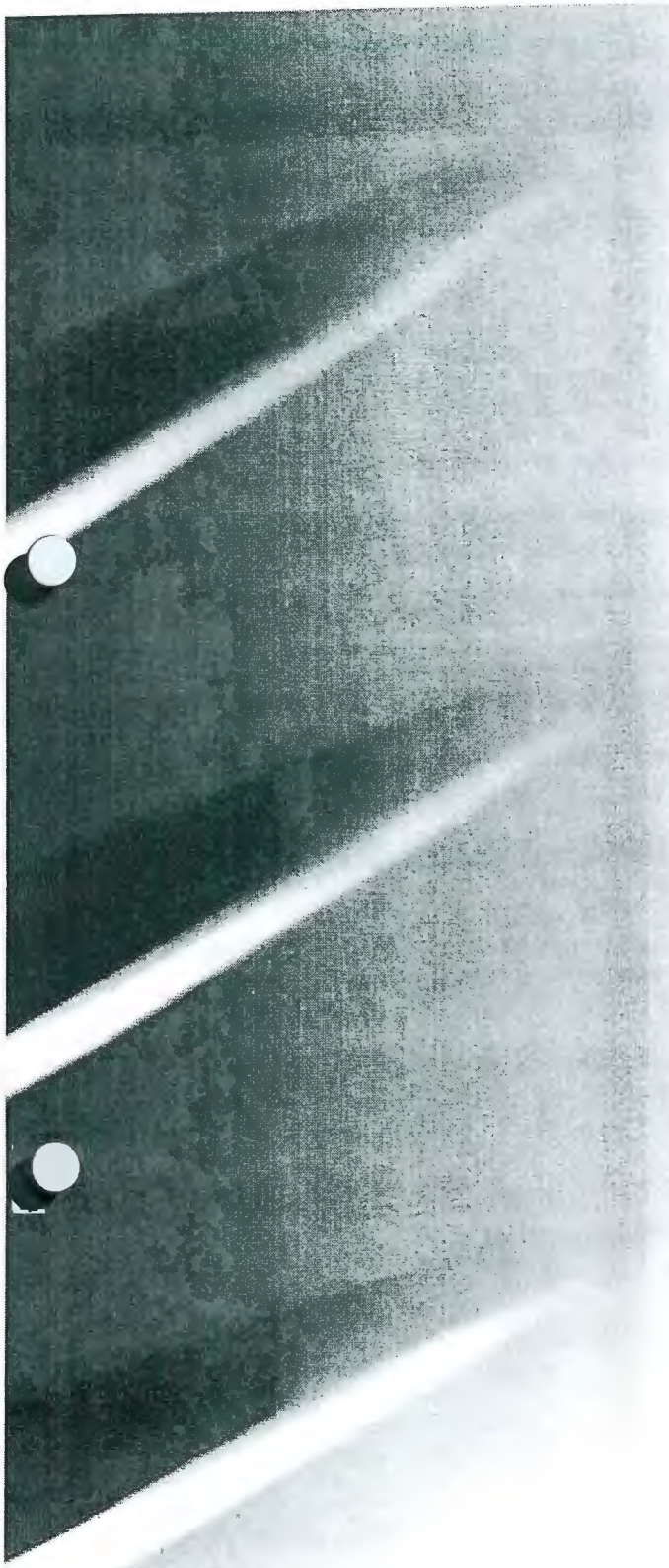
Index

U

W

ANEXO SWITCH TIPO 03
PARTE 6

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br



EMC Connectrix
Departmental Switch DS-32B2 and Enterprise Director ED-12000B
Fabric OS
Version 4.1

PROCEDURES MANUAL

P/N 300-000-638
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

Connectrix B Series systems have been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio-frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Preface

The EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric OS Procedures Manual provides procedures for many of the basic tasks of administrating and configuring a ED-12000B switch through the Telnet interface. For tasks related to specific features such as zoning, refer to the individual product guides.

If an EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B feature does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

This manual is part of the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B documentation set, and is intended for use by administrators of the DS-32B2 and ED-12000B switches.

Readers of this manual are expected to be familiar with the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B operating environment.

Organization

Here is an overview of where information is located in this manual.

- Chapter 1, *Setting the Initial Configuration*, provides information on initial configuration procedures including logging in and changing passwords.
- Chapter 2, *Basic Configuration Procedures*, provides information on basic configuration procedures.
- Chapter 3, *Standard Security in Fabric OS*, provides information regarding security features that are standard in the Fabric OS.

- Chapter 4, *Working With ED-12000B*, provides information on working with the Management Server platform database.
- Chapter 5, *Working With the Management Server*, provides information about working with the Management Server platform database.
- Chapter 6, *Diagnostics and Status*, provides instructions for displaying port and switch status information.
- Chapter 7, *Updating the Core PID Format*, provides information about updating the Core Switch Port Identifier (PID) Format, including best practices for updating an existing production SAN to the new PID format.
- Chapter 8, *Troubleshooting*, provides information on troubleshooting and the most common procedures used to diagnose and repair issues. In this chapter
- Appendix A, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B.
- The *Glossary* defines terminology used in this manual.

Related Documentation

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*

- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Manual

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this manual:

Palatino, bold	• Dialog box, button, icon, and menu items in procedures • Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	• New terms or unique word usage in text • Command line arguments when used in text • Book titles
Courier, italic	Arguments used in examples of command line syntax.

Courier	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

Courier, bold	User entry. For example: `symmpoll -p`
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC website at:

`http://www.EMC.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.EMC.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to **techpub_comments@EMC.com** with your opinions of this manual.

1 Setting the Initial Configuration

The EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B requires two connections to your IP network. This chapter provides information on how to set up initial configuration tasks for a switch.

Configuring and Managing the Switch

For specific switch installation and configuration instructions, refer to the hardware manual for your switch. Setting up and configuring the switch involves the following steps:

- Obtaining IP addresses, subnet masks, and gateway addresses from the network administrator.

  For the ED-12000B, you will need four IP addresses.

- Installing and powering on the switch.
- Creating a serial connection to the switch from a workstation computer that has a terminal emulator application (such as HyperTerminal).
- Configuring the IP address (required to prevent IP conflict) and other settings.
- Creating an ethernet connection to the switch.
- Connecting the switch to the fabric.

After the switch is configured and connected to the network and fabric, you can use any of the following methods to manage the switch:

- Fabric OS command line interface (CLI), through a serial or telnet connection
- Web Tools
- Standard SNMP applications
- Through a third-party application using the API
- Through a third-party application using the Management Server

In general, switch administration should be performed from the admin user level.

Logging in to a Switch

To avoid an IP address conflict, do NOT connect the switch to the IP network until the IP address is correctly set. For instructions on setting the IP address and connecting to the network, refer to the hardware reference manual for your switch.

To log in to a DS-32B2 or ED-12000B switch:

1. Open a connection to the switch:
   - Serial: Connect the switch and workstation by serial cable, then open and configure a terminal emulator application according to the settings provided in the hardware manual.
   - Telnet: Connect the switch and workstation by ethernet cable, then use the configured IP address to open a telnet connection to the switch.
2. Enter the admin login.

   The password prompt displays.
3. Enter the admin password.

   When you first log in to a switch as the admin user, you are prompted to change the passwords for all user levels. This prompt continues to display until the passwords are modified.
4. If the login is successful, a prompt that contains both the switch name and the login displays.

Example

```
switch login: admin
Password: xxxxxxxx
Please change your passwords now.
Use Control-C to exit or press 'Enter' key to proceed.

Please change your passwords now.
for user - admin
Changing password for admin
Enter new password:xxxxxxxx
Reenter password:xxxxxxxx
switch:admin>
```

Set the Boot PROM and Recovery Passwords

About the Boot Prom and Recovery Passwords

The Boot PROM and Recovery passwords provide an additional layer of security beyond the Root password.

- Setting a Boot PROM password protects the boot prompt from unauthorized use.
- Setting a Recovery password turns on the password recovery option, which requires a user to contact EMC Technical Support before recovering a Root or Boot PROM password.

CAUTION

Setting both the Boot PROM and Recovery passwords on all switches running Fabric OS v4.1.0 is strongly recommended. Not setting either of these passwords can compromise fabric security.

Setting the Boot PROM and the Recovery Passwords (DS-32B2)

To set the Boot PROM password without setting the Recovery password, refer to <Italic>Setting the Boot PROM Password Only (DS-32B2).

Setting the Boot PROM and Recovery passwords requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

1. Connect to the serial port interface as described in <Italic>Setting the Boot PROM Password Only (DS-32B2).
2. Reboot the switch.
3. Press **ESC** within four seconds after the message "Press escape within 4 seconds..." displays.
4. The following options are available:
   - Start system.
   - Recovery password.
   - Enter command shell.
5. Enter "2" at the prompt to set the Recovery password.
   The following message displays: "Recovery password is NOT set. Please set it now."

6. Enter the Recovery password.
   The Recovery password must be between 8 and 40 alphanumeric characters. A random password that is 15 characters or longer is recommended for higher security. The firmware only prompts for this password once. It is not necessary to remember the Recovery password.
7. The prompt for the Boot PROM password displays: "New password:".
8. Enter the Boot PROM password, then re-enter when prompted. Record this password for future use.
9. The new passwords are automatically saved (**saveenv** command not required).
10. Reboot the switch.
    Traffic flow resumes when the switch finishes rebooting.

CAUTION

It is extremely important that you note and safely store the boot prom password. The password may be required to troubleshoot a specific situation, so having the password available can save valuable time. Recovering the password is a time-consuming process, and requires contacting EMC Technical Support.

Setting the Boot PROM and Recovery Passwords (ED-12000B)

To set the Boot PROM password without setting the Recovery password, refer to <Italic>Setting the Boot PROM Password Only (ED-12000B).

The Boot PROM and Recovery passwords must be set for each CP card on an ED-12000B switch.

1. Connect to the serial port interface on the standby CP card, as described in *Setting Both the Boot PROM and Recovery Passwords (ED-12000B)* on page 3-28.
2. Log in to the active CP card by serial or telnet and enter the **hadisable** command to prevent failover during the remaining steps.
3. Reboot the Standby CP card by pressing the yellow ejector buttons at top and bottom of the CP card, then pressing both ejector handles back towards the switch to lock the card back into the slot.

4. Press **ESC** within four seconds after the message "Press escape within 4 seconds..." displays.
5. The following options are available:
   - Start system.
   - Recovery password.
   - Enter command shell.
6. Enter "2" at the prompt to set the Recovery password.
   The following message displays: "Recovery password is NOT set. Please set it now."
7. Enter the Recovery password.
   The Recovery password must be between 8 and 40 alphanumeric characters. A random password that is 15 characters or longer is recommended for higher security. The firmware only prompts for this password once. It is not necessary to record the Recovery password.
8. The following prompt displays: "New password:".
9. Enter the Boot PROM password, then re-enter when prompted. Record this password for future use.
10. The new passwords are automatically saved (**saveenv** command not required).
11. Failover the active CP card by entering the **hafailover** command. Traffic flow through the active CP card resumes when the failover is complete.
12. Connect the serial cable to the serial port on the new standby CP card (previous active CP card).
13. Repeat step 2 through step 10 for the new standby CP card (each CP card has a separate Boot PROM password).
14. Log in to the active CP card by serial or telnet and enter the **haenable** command to restore high availability.

CAUTION

It is extremely important that you note and safely store the boot prom password. The password may be required to troubleshoot a specific situation, so having the password available can save valuable time. Recovering the password is a time-consuming process, and requires contacting EMC Customer Support.

Customize the Switch Name

You can customize the switch names for the logical switches. If you chose to change the default switch name, use a switch name that is unique and meaningful.

Changing the switch name causes a domain address format RSCN to be issued.

Switch names:

- can be up to 15-characters long for v4.1.0
- can be up to 19-characters long for v3.1
- must begin with an alpha character
- can consist of any combination of alphanumeric and underscore characters

Default Names

The default names for the ED-12000B are "sw0" for the switch containing the port cards in slots 1-4, and "sw1" for the switch containing port cards in slots 7-10.

Customizing a Switch Name

To customize the switch name:

1. Verify the CP to which the serial cable is connected.
2. Log in to the switch as admin.
3. (*For ED-12000B switches only*) Choose the logical switch that you want to change. Enter the value that corresponds to that logical region:
   - Enter 0 to configure logical switch 0 (slot 1 through 4)
   - Enter 1 to configure logical switch 1 (slot 7 through 10)
4. Enter the **switchname** command.
5. Enter the new name in quotes, as shown in the following example:

```
switchname "sw10"
```

For more information about this command, refer to the *Fabric OS Reference Guide*.

6. Record the new switch name for future reference.

7. (Optional) Log out of the CP session, and repeat steps 1 - 6 for the 2nd logical switch.

Enabling Licensed Features

Optional licensed features such as Fabric Watch and Performance Monitoring are already loaded onto the switch firmware, but you must enable them with a license key. Once you purchase these features, you receive a transaction key to unlock the feature.

Important You must log on to Powerlink or contact EMC Customer Support to convert the transaction key to a license key.

Displaying the Installed Feature Licenses

To display the features that have been enabled on a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `licenseShow`

   This command displays the license keys that have been entered for the switch and the features enabled by those licenses.

Example

```
Licenseshow output:licenseshow
cy99QyeebrzAARk:
    Web license
    Zoning license
    Fabric license
    Extended Fabric license
    Fabric Watch license
    Performance Monitor license
    Trunking license
```

Changing the Admin Password

EMC recommends that you change the admin and user ID and password the first time you log in to the Fabric Operating System.

To change the admin user password:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `Passwd admin` (to change admin password); or

   `Passwd user` (to change user password)
3. An interactive session opens and prompts you for configuration values.
   a. At the **New password** prompt, enter the new password. The new password must be from 8 to 40 characters in length.
   b. At the **Reenter new password** prompt, enter the new password exactly as entered at the previous prompt.
   c. Press ENTER to commit the configuration to the firmware.

Configuring the IP Address

Configuring the IP Address on the ED-12000B

For ED-12000B only:
The ED-12000B switch ships with a default IP address of:
CP0 - 10.77.77.75, CP1 - 10.77.77.74, SW0 - 10.77.77.77, and SW1 - 10.77.77.76 .

To change the default IP Address and configure the Fibre Channel IP address of the switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `ipAddrSet`

3. Choose the logical switch or CP that you want to configure. Enter the value that corresponds to that logical region:
   - Enter **0** to configure logical switch 0 (slot 1 through 4)
   - Enter **1** to configure logical switch 1 (slot 7 through 10)
   - Enter **2** to configure control processor 1 (slot 5)
   - Enter **3** to configure control processor 2 (slot 6)
4. If you are configuring a logical switch, enter the following information when prompted:
   - Ethernet IP Address
   - Ethernet Subnetmask
   - Fibre Channel IP Address
   - Fibre Channel Subnetmask
5. If you are configuring a control processor, enter the following information when prompted:
   - Ethernet IP Address
   - Ethernet Subnetmask
   - Hostname
   - Gateway IP Address
6. Once you have configured a logical switch or control processor, the `ippaddrset` command verifies the data you entered, and exits.
7. Rerun this command to configure all logical switches and control processors.

8. Optional: Verify the address was correctly set by entering the `ipAddrShow` command at the prompt and enter option 4 (4 for all IP addresses in the system). This will display the IP address setting for both switches and both CP cards.

Configuring the IP Address on a DS-32B2

To change the default IP Address and configure the Fibre Channel IP address of the switch:

1. Log in to the switch as the admin user.
2. Replace the factory IP address and related information with the IP information provided by your network administrator:
   a. Enter the `ipAddrSet` command at the terminal emulator application prompt.
   b. Enter the requested information at the prompts:
      - `Ethernet IP Address [10.77.77.77]:`
        Enter the new Ethernet IP address.
      - `Ethernet Subnetmask [255.0.0.0]:`
        Enter the new Ethernet subnet mask.
      - `Fibre Channel IP Address [0.0.0.0]:`
        Enter the new Fibre Channel IP address if desired.
      - `Fibre Channel Subnetmask [0.0.0.0]:`
        Enter the new Fibre Channel subnet mask if desired.
      - `Gateway Address [0.0.0.0]:`
        Enter the new gateway address.
      - `Set IP address now? [y = set now, n = next reboot]:`
        Enter `y` to set now.
   c. Optional: Verify the address was correctly set by entering the `ipAddrShow` command at the prompt.

Selecting the Slot and Port for the ED-12000B

Many commands used to administer ports in the ED-12000B require you to specify the slot number and port number operands. These operands are used to identify individual ports on the switch.

The slotnumber operand must be followed by the slash (/) and then a value for the port number:

```
portEnable 2/4
```

The ED-12000B has a total of 10 slots counted 1 to 10. Slot number 5 and 6 are control processor cards, and slot 1 through 4, and 7 through 10 are switch cards. On each switch card, there are 16 ports counted from the bottom 0 to 15. A particular port must be represented by both slotnumber (1 through 10) and portnumber (0 through 15). This operand is not required for switches that do not have blades.

Understanding the Core PID Requirements

Core PID addressing is an option of the **configure** command for 2.6.0c + and 3.0.2.g+ firmware, but *not* 4.x firmware. However, even if you are configuring a ED-12000B or DS-32B2 switch, it is important to note this requirement if you have a fabric that mixes 4.x switches with other switches. Failing to update the Core PID addressing in non-4.x switches will result in segmentation in a mixed fabric.

For detailed information regarding Core PID and related procedures, refer to Chapter 7, *Updating the Core PID Format*.

For fabrics that consist of only 4.x.x firmware (12000 or DS-32B2 switches), no action is required to configure the Core PID. The Core PID is enabled by default, and this parameter cannot be changed. However, other switches in your fabric will need to be Core PID enabled *if* you mixing 2.x.x or 3.x.x. firmware with your 4.x.x firmware in a single fabric.

Mixed Fabric Requirements

To mix 2.x.x or 3.x.x switches in to a fabric that contains one or more 4.x.x switches, the following is required:

Minimum Firmware

- 2.x.x firmware must be 2.6.0c + (though 2.6.1 is strongly recommended for full functionality)
- 3.x.x firmware must be 3.0.2g

Configuration Requirement

- The Core PID must be enabled on all 2.6.0c + and 3.0.2g + switches. Refer to <Italic>(Optional) Enabling Core PID Addressing.

(Optional) Enabling Core PID Addressing

To enable Core PID addressing on 2.6.0c or 3.0.2g switches for the purpose of mixing in to a 4.x.x fabric:

1. Telnet in to the switch.
2. Log in to the switch as admin.
3. Disable the switch by entering the **switchdisable** command.
4. Enter the **configure** command (the configure prompts display sequentially).
5. Enter "y" after the "Fabric parameters" prompt. Be sure to use the same configuration parameters as the rest of your fabric.

6. Enter "1" at the "Core Switch PID Format" prompt.This enables the Core PID addressing, and allows the non-4.x switch to merge in to a 4.x fabric.
7. Complete the remaining prompts, or press CTRL-D to accept the remaining settings without completing all the prompts.
8. Be sure to use the same configuration parameters as the rest of your fabric.
9. Repeat steps 1 - 4 for all 2.6.0c or 3.0.2g switches that you want to incorporate in to the mixed fabric.

Verifying the Switch Operation

To verify that your switch is operating correctly, display information about the switch and port status.

To display information about the switch and port status:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   switchshow

   This command displays a switch summary and a port summary.

   The following example shows a DS-32B2:

```
switch32:admin> switchshow
switchName:     switch32
switchType:     12.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:60:69:90:03:56
switchBeacon:   OFF

Port Gbic Speed State
==========================
  0   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  1   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  2   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  3   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  4   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  5   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32" (downstream)
  6   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  7   id    N2   Online    E-Port  10:00:00:60:69:c0:05:f4 "switch32"
  8   id    N2   No_Light
  9   id    N2   No_Light
 10   id    N2   No_Light
 11   id    N2   No_Light
 12   id    N2   No_Light
 13   id    N2   No_Light
 14   id    N2   No_Light
 15   id    N1   Online    E-Port  10:00:00:60:69:30:2f:2f "fmgr25_2010" (upstream)
 16   id    N2   No_Light
 17   id    N2   No_Light
 18   id    N2   No_Light
 19   id    N2   No_Light
 20   id    N2   No_Light
 21   id    N2   No_Light
 22   id    N2   No_Light
```

```
 23   id    N2   No_Light
 24   id    N2   No_Light
 25   id    N2   No_Light
 26   id    N2   No_Light
 27   id    N2   No_Light
 28   id    N2   No_Light
 29   id    N2   No_Light
 30   id    N2   No_Light
 31   id    N2   No_Light
switch32:admin>
```

The following example shows an ED-12000B:

```
switch12k:admin> switchshow
switchName:switch12k
switchType:10.1
switchState:Online
switchRole:Subordinate
switchDomain:2
switchId:fffc02
switchWwn:10:00:00:60:69:50:02:8f
switchBeacon:OFF
blade7: Beacon: OFF
Area Slot Port SFP Speed State
=====================================
 0    7    0   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
   (downstream)
 1    7    1   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
 2    7    2   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
 3    7    3   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
 4    7    4   id    N1   Online    E-Port  10:00:00:60:69:12:34:e2 "san180"
 5    7    5   id    1G   No_Light
 6    7    6   --    1G   No_Module
 7    7    7   --    1G   No_Module
 8    7    8   --    1G   No_Module
 9    7    9   id    N2   Online    F-Port  21:00:00:e0:8b:04:1a:76
10    7   10   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
11    7   11   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
12    7   12   --    1G   No_Module
13    7   13   --    1G   No_Module
14    7   14   id    N1   Online    E-Port  10:00:00:60:69:10:9b:06 "san176"
   (upstream)
15    7   15   id    N2   Online    F-Port  10:00:00:00:c9:27:2e:69
switch12k:admin>
```

Verify Hi-Availability (HA)

1. Log in to the switch (if not already logged in).
2. Enter the **hashow** command.

Verify that HA is enabled, that the heartbeat is up, and that the HA is in sync.

```
switch:admin> hashow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State is in sync
```

3. (Optional) Enter the **chassishow** command to verify operation of the Field Replaceable Units (FRUs).

Example:

```
switch12k:admin> chassisshow

SW BLADE Slot: 3
Header Version: 1
Power Consume Factor: -180
Brocade Part Num: 60-0001532-03
Brocade Serial Num: 1013456800
Manufacture: Day: 12 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 28 days
Time Awake: 16 days
ID: 555-374757q> to stop
Part Num: 234-294-12345
Serial Num: 2734658
Revision Num: A.00

CP BLADE Slot: 6
Header Version: 1
Power Consume Factor: -40
Brocade Part Num: 60-0001604-02
Brocade Serial Num: FP00X600128
Manufacture: Day: 12 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 61 days
Time Awake: 16 days
ID: 555-374757
Part Num: 236-296-12350
Serial Num: 2836542
Revision Num: A.00

POWER SUPPLY Unit: 2
Header Version: 1
Power Consume Factor: 1000
Brocade Part Num: 60-0001536-02to stop
Brocade Serial Num: A013450700
Manufacture: Day: 14 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 50 days
Time Awake: 16 days
ID: 555-374757
Part Num: 238-298-12360
Serial Num: 1234567

<output truncated>
```

4. (Optional) Enter the **slotshow** command to inventory and display the current status of each slot in the system.

Example:

```
switch:admin> slotshow

Slot Blade Type ID Status
---------------------------------
1 SW BLADE 2 FAULTY
2 SW BLADE 2 DISABLED
3 SW BLADE 2 ENABLED
4 SW BLADE 2 DIAG RUNNING POST2
5 CP BLADE 1 ENABLED
6 CP BLADE 1 ENABLED
7 UNKNOWN VACANT
8 SW BLADE 2 DIAG RUNNING POST1
9 SW BLADE 2 INSERTED, NOT POWERED ON
10 UNKNOWN VACANT
```

Connect ISLs to Switch

Refer to the *Hardware User's Guide* of your specific switch for ISL connection and cable management information.

Verifying the Fabric Connectivity

To verify that you have fabric-wide switch connectivity, display a summary of information about the fabric:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   fabricshow

This command displays a summary of all the switches in the fabric:

```
switch:admin> fabricShow

   Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr      Name
   -------------------------------------------------------------------------
    3: fffc43 10:00:00:60:69:10:60:1f  192.168.64.187  0.0.0.0         "sw187"
    2: fffc42 10:00:00:60:69:00:05:91  192.168.64.60   192.168.65.60   "sw60"
    1: fffc41 10:00:00:60:69:00:02:0b  192.168.64.180  192.168.65.180 >"sw180"
    0: fffc40 10:00:00:60:69:00:06:56  192.168.64.59   192.168.65.59   "sw5"

   The Fabric has 4 switches
```

Verify Hi-Availability (HA)

1. Log in to the switch (if not already logged in).
2. Enter the **hashow** command.

   Verify that HA is enabled, that the heartbeat is up, and that the HA is in sync.

Example

```
switch:admin> hashow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State is in sync
```

3. (Optional) Enter the **chassishow** command to verify operation of the Field Replaceable Units (FRUs).

```
switch12k:admin> chassisshow

SW BLADE Slot: 3
Header Version: 1
Power Consume Factor: -180
Brocade Part Num: 60-0001532-03
Brocade Serial Num: 1013456800
Manufacture: Day: 12 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 28 days
Time Awake: 16 days
ID: 555-374757q> to stop
Part Num: 234-294-12345
Serial Num: 2734658
Revision Num: A.00

CP BLADE Slot: 6
Header Version: 1
Power Consume Factor: -40
Brocade Part Num: 60-0001604-02
Brocade Serial Num: FP00X600128
Manufacture: Day: 12 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 61 days
Time Awake: 16 days
ID: 555-374757
Part Num: 236-296-12350
Serial Num: 2836542
Revision Num: A.00

POWER SUPPLY Unit: 2
Header Version: 1
Power Consume Factor: 1000
Brocade Part Num: 60-0001536-02to stop
Brocade Serial Num: A013450700
Manufacture: Day: 14 Month: 6 Year: 2001
Update: Day: 15 Month: 7 Year: 2001
Time Alive: 50 days
Time Awake: 16 days
ID: 555-374757
Part Num: 238-298-12360
Serial Num: 1234567

<output truncated>
```

4. (Optional) Enter the **slotshow** command to inventory and display the current status of each slot in the system.

```
switch:admin> slotshow

Slot Blade Type ID Status
---------------------------------
1 SW BLADE 2 FAULTY
2 SW BLADE 2 DISABLED
3 SW BLADE 2 ENABLED
4 SW BLADE 2 DIAG RUNNING POST2
5 CP BLADE 1 ENABLED
6 CP BLADE 1 ENABLED
7 UNKNOWN VACANT
8 SW BLADE 2 DIAG RUNNING POST1
9 SW BLADE 2 INSERTED, NOT POWERED ON
10 UNKNOWN VACANT
```

Verifying the Fabric-Wide Device Count

To verify that you have fabric-wide connectivity when you install a new switch, display the fabric-wide device count from the newly installed switch.

To display the fabric-wide device count from a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   nsAllShow

   This command displays all the connected devices in the fabric:

```
switch:admin> nsAllShow

   17 Nx_Ports in the Fabric {
  190000 1907da 1907dc 1907e0 1907e1 1907e2 1907e4 1907e8
  1907ef 1a07da 1a07dc 1a07e0 1a07e1 1a07e2 1a07e4 1a07e8
  1a07ef
}
switch:admin>
```

Connect Devices to the Switch

Power off all devices (to minimize PLOGIs) and connect them to the switch, according to your topology. For devices that cannot be powered off, connect the devices, but use the **portdisable** command to disable the port on the switch.

When powering the devices back on, wait for each device to complete the fabric login before powering on the next one.

Verifying Device Connectivity

To view and verify that you have fabric-wide device connectivity, display the fabric wide device count. The number of devices listed in the Name Server (NS) should reflect the number of devices that are connected.

1. Log in to the switch as the admin user.
2. (Optional) Enter the **switchshow** command to verify that the storage devices are logged in.
3. (Optional) Enter the **nsshow** command to verify that the storage devices have successfully registered with the Name Server.
4. Enter the **nsallshow** command at the command line. This command displays 24-bit fibre channel addresses of all devices in the fabric.

```
switch:admin> nsallshow
75 Nx_Ports in the Fabric {
  010e00 012fe8 012fef 030500 030b04 030b08 030b17 030b18
  030b1e 030b1f 040000 050000 050200 050700 050800 050de8
  050def 051700 061c00 071a00 073c00 090d00 0a0200 0a07ca
  0a07cb 0a07cc 0a07cd 0a07ce 0a07d1 0a07d2 0a07d3 0a07d4
  0a07d5 0a07d6 0a07d9 0a07da 0a07dc 0a07e0 0a07e1 0a0f01
  0a0f02 0a0f0f 0a0f10 0a0f1b 0a0f1d 0b2700 0b2e00 0b2fe8
  0b2fef 0f0000 0f0226 0f0233 0f02e4 0f02e8 0f02ef 210e00
  211700 211fe8 211fef 2c0000 2c0300 611000 6114e8 6114ef
  611600 620800 621026 621036 6210e4 6210e8 6210ef 621400
  621500 621700 621a00
}

switch:admin>
```

Backing Up Critical Switch Information

EMC recommends two types of backups: a print out of all key configuration data, stored in a secure location, and regularly scheduled soft copy backups.

For information about creating a backup of configuration data, refer to *Backing Up the System Configuration Settings* on page 2-6.

EMC recommends that you make a hard copy backup of all key configuration data, including license key information, and store it in a secure place for emergency reference.

Store the output of the following commands in a secure location:

- `licenseshow`
- `configshow`
- `ipaddrshow` - (For the ED-12000B only. Select option 4 to display all configured addresses)
- `configupload`

Depending on the security procedures of your company, you may want to keep a record of the user levels and passwords for all switches in the fabric. This is sensitive information and access to such information should be limited.

2

Basic Configuration Procedures

This chapter provides the following information on basic configuration tasks for the DS-32B2 and ED-12000B switches:

Setting the Telnet Time Out Value

To set a new Telnet time out value:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `timeout x`

   where `x` is the number of minutes before the Telnet connection times out. If you specify `0`, then the connection never times out. Time out is disabled by default.

Displaying the Firmware Version

To display the firmware version:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `version`

   This command displays the Kernel version, Fabric OS release number, and other information about the firmware.

   The following example shows the firmware version information:

```
switch:admin> version
Kernel:      2.4.2
Fabric OS:   v4.0.2a
Made on:     Tue Aug 13 11:15:32 2002
Flash:       Tue Aug 13 19:15:01 2002
BootProm:    3.1.18
switch:admin>
```

Setting the Switch Date and Time

All switches maintain current date and time in nonvolatile memory. Date and time are used for logging events. Switch operation does not depend on the date and time; a switch with an incorrect date and time value still functions properly.

To set the date and time of a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `date MMDDhhmmYY`

   where:

   `MM` is the month, valid values are `01 through 12`.

   `DD` is the day, valid values are `01 through 31`.

   `hh` is the hour, valid values are `00 through 23`.

   `mm` is minutes, valid values are `00 through 59`.

   `YY` is the year, valid values are `00 through 99`.

Year values greater than 69 are interpreted as 1970 through 1999; year values less than 70 are interpreted as 2000 through 2069. The date function does not support daylight savings time or time zones.

Correct the Time Zone of a Switch

If the time of your switch(es) is off by hours (and not minutes), use the following procedure on all switches to set the Time Zone.

1. Log in as admin.
2. Enter the **tstimezone** command as follows:

   tstimezone [*houroffset* [, *minuteoffset*]]

Example

- For Pacific Standard Time enter **tsTimeZone -8,0**
- For Central Standard Time enter **tsTimeZone -6,0**
- For Eastern Standard Time enter **tsTimeZone -5,0**

The default time zone for switches is Universal Time Conversion (UTC), which is 8 hours ahead of Pacific Standard Time. For additional time zone conversions, refer to <Italic>Direct Conversions from UTC to Local Time below.

The parameters listed above would not apply if the time zone of the switch(es) has already been changed from the default (8 hours ahead of PT).

Refer to the **tstimezone** command in the *Fabric OS Reference Guide* for more detailed information about the command parameters.

3. Repeat steps 1 and 2 on all switches for which the Time Zone needs to be set.

   This only needs to be done once because the value is written to flash.

Direct Conversions from UTC to Local Time

Use the following information to determine the correct parameter for the **tstimezone** command.

Table 2-1 Direct Conversions from UTC to Local Time

Local Time	Subtract from UTC
Atlantic Standard	-4,0
Atlantic Daylight	-3,0
Eastern Standard	-5,0
Eastern Daylight	-4,0

Table 2-1 Direct Conversions from UTC to Local Time (*continued*)

Local Time	Subtract from UTC
Central Standard	-6,0
Central Daylight	-5,0
Mountain Standard	-7,0
Mountain Daylight	Six hours
Pacific Standard	Eight hours
Pacific Daylight	Seven hours
Alaskan Standard	Nine hours
Alaskan Daylight	Eight hours
Hawaiian Standard	Ten hours

Backing Up the System Configuration Settings

This procedure requires access to an FTP server for Fabric OS 4.x, and an FTP or RSHD server for Fabric OS 3.x.

Fabric OS version 4.x does not support the RSH protocol for uploads or downloads. Therefore, you must use the FTP protocol on all workstations to backup or restore the system configuration, and the FTP service must be running before an upload or download can occur.

To upload a backup copy of the configuration settings to a host computer:

1. Verify that the FTP service is running on the host workstation.
2. Log in to the switch as the admin user.
3. At the command line, enter the following command:

   `configUpload`

   You are prompted for the required information.
4. Provide the information requested at the prompts. This command uploads the switch configuration to the designated server, making it available for downloading to a replacement switch if necessary.

   This command uploads the switch configuration to the designated server, making it available for downloading to a replacement switch if necessary.

EMC recommends backing up the switch configuration to a host computer on a regular basis. This ensures that a fairly current configuration is available if required for downloading to a replacement switch.

All filenames/pathnames must be in UNIX syntax even if being executed from a Windows-based system (i.e., `/temp/switch_2.txt`).

Example

```
switch:admin> configupload
   Server Name or IP Address [host]: 192.168.15.42
   User Name [None]: user21
   File Name [config.txt]: config-switch.txt
   Password: xxxxxx
   upload complete
   switch:admin>
```

Displaying the System Configuration Settings

To display the system configuration settings:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `configShow`

   The system configuration settings appear.

System configuration parameters vary depending on switch model and configuration.

Restoring the System Configuration Settings

You must use the FTP protocol on all workstations to backup or restore the system configuration, and the FTP service must be running before an upload or download can occur.

To restore the system configuration settings from a backup:

1. Verify that the FTP service is running on the host workstation.
2. Log in to the switch as the admin user.
3. Shut down the switch by entering the following command:

   ```
   switchDisable
   ```

4. At the command line, enter the following command:

   ```
   configdownload
   ```

   The command becomes interactive and you are prompted for the required information.

   For example:

   ```
   switch:admin> configdownload
      Server Name or IP Address [host]: 192.168.15.42
      User Name [None]: user21
      File Name [config.txt]: config-file.txt
      Password: xxxxxx
      download complete
      switch:admin>
   ```

5. Reboot the switch by entering the following command:

   ```
   switchreboot
   ```

Disabling a Switch

To disable a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
switchDisable
```

All Fibre Channel ports on the switch are taken off line. If the switch was part of a fabric, the remaining switches reconfigure.

Enabling a Switch

To enable a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
switchEnable
```

All Fibre Channel ports that passed the POST test are enabled. If the switch was part of a fabric, the switch rejoins the fabric.

Disabling a Port

To disable a port:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
portDisable [slotnumber/]portnumber
```

The slotnumber applies only to ED-12000B.

where `slotnumber` and `portnumber` are the slot and port number you want to disable. If the port is connected to another switch, the fabric may reconfigure. If the port is connected to one or more devices, these devices are no longer available to the fabric.

The following example shows the `portdisable` command on a DS-32B2, where 1 is the portnumber.

```
switch:admin> portdisable 1
fabric: Reconfiguration due to offline (port 1)
fabric: Reconfiguring (Mon Aug  5 10:51:19 2002)
 5  4  3  2  1

fabric: Subordinate switch
fabric: Domain 52

switch:admin>
```

The following example shows the `portdisable` command on an ED-12000B, where 7 is the slotnumber and 3 is the portnumber.

```
switch12k:admin> portdisable 7/3
switch12k:admin> portshow 7/3
portCFlags: 0x0
portFlags: 0x20801       PRESENT DISABLED LED
portType:  4.1
portState: 2    Offline
portPhys:  6    In_Sync
portScn:   2    Offline
<output truncated>
```

Enabling a Port

To enable a port:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   portEnable [slotnumber/]portnumber

   where `slotnumber` and `portnumber` are the slot and port number you want to enable. If the port is connected to another switch, the fabric may reconfigure. If the port is connected to one or more devices, these devices will become available on the fabric.

   The slotnumber applies only to ED-12000B.

The following example shows the `portenable` command on a DS-32B2.

```
switch:admin> portenable 1
switch:admin> portshow 1
portCFlags: 0x1  ENABLED
portFlags: 0x228057     PRESENT ACTIVE E_PORT G_PORT U_PORT LOGIN LED
   ACCEPT
portType:  4.1
portState: 1    Online
portPhys:  6    In_Sync
portScn:   5    E_Port
portId:    010100
portWwn:   20:01:00:60:69:90:03:56
portWwn of device(s) connected:
        None
Distance:  normal
Speed: N2Gbps

Interrupts:         20835     Link_failure: 52        Frjt:          0
Unknown:            46        Loss_of_sync: 1820      Fbsy:          0
Lli:                1992       Loss_of_sig:  3
Proc_rqrd:          18832      Protocol_err: 0
Timed_out:          0          Invalid_word: 0
Rx_flushed:         0          Invalid_crc:  0
Tx_unavail:         0          Delim_err:    0
Free_buffer:        0          Address_err:  0
Overrun:            0          Lr_in:        53
Suspended:          0          Lr_out:       38
Parity_err:         0          Ols_in:       33
2_parity_err:       0          Ols_out:      8
CMI_bus_err:        0
switch:admin>
```

The following example shows the `portenable` command on an ED-12000B, where 7 is the slotnumber and 3 is the portnumber.

```
switch12k:admin> portenable 7/3
switch12k:admin> portshow 7/3
portCFlags: 0x1
portFlags: 0x23801b      PRESENT ACTIVE F_PORT G_PORT LOGIN NOELP LED
   ACCEPT
portType:  4.1
portState: 1    Online
portPhys:  6    In_Sync
portScn:   6    F_Port
<output truncated>
```

Changing a Switch Name

To change the name of a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `switchName new_name`

   where `new_name` is the new name for the switch. Switch names can be up to 19 characters long, must begin with a letter, and can contain letters, numbers, or the underscore character.

Setting the Switch Status Policy

There are seven parameters that determine the status of a switch:

- Number of faulty ports
- Missing GBICs (such as, Small Form Factor Pluggable (SFP) transceivers)

  GBIC and SFP are interchangeable terms.

- Power supply status
- Temperature in enclosure
- Fan speed
- Port status
- sgroup ISL status

Each parameter can be adjusted so that a specific threshold must be reached before that parameter changes the overall status of a switch to MARGINAL or DOWN. Only one parameter needs to pass the MARGINAL or DOWN threshold to change the overall status of the switch.

Important Do not modify these parameters unless so notified by EMC Customer Service.

Viewing the Policy Threshold Values

To view the switchStatusPolicy threshold values:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
switch:admin> switchStatusPolicyShow
```

The following output displays:

```
switch:admin> switchStatusPolicyShow
The current overall switch status policy parameters:
```

	Down	Marginal
FaultyPorts	2	1
MissingGBICs	0	0
PowerSupplies	2	1
Temperatures	2	1
Fans	2	1
PortStatus	0	0
sgroup ISLStatus	0	0

```
switch:admin>
```

Configuring the Policy Threshold Values

To set the switch status policy threshold values:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
switchStatusPolicySet
```

The current switch status policy parameter values are displayed.

3. You are prompted to enter values for each parameters DOWN and MARGINAL threshold:
   - Enter the number of faulty ports required to change the switch status to DOWN and press ENTER.
   - Enter the number of faulty ports required to change the switch status to MARGINAL and press ENTER.

- Enter the number of missing GBICs required to change the switch status to DOWN and press ENTER.
- Enter the number of missing GBICs required to change the switch status to MARGINAL and press ENTER.
- Enter the number of bad Power Supply warnings required to change the switch status to DOWN and press ENTER.
- Enter the number of bad Power Supply warnings required to change the switch status to MARGINAL and press ENTER.
- Enter the number of temperature warnings required to change the switch status to DOWN and press ENTER.
- Enter the number of temperature warnings required to change the switch status to MARGINAL and press ENTER.
- Enter the number of fan speed warnings required to change the switch status to DOWN and press ENTER.
- Enter the number of fan speed warnings required to change the switch status to MARGINAL and press ENTER.
- Enter the number of port down warnings required to change the switch status to DOWN and press ENTER.
- Enter the number of port down warnings required to change the switch status to MARGINAL and press ENTER.
- Enter the number of ISLstatus down warnings required to change the switch status to DOWN and press ENTER.
- Enter the number of ISLstatus down warnings required to change the switch status to MARGINAL and press ENTER.

4. Verify the threshold settings you have configured for each parameter. Enter the following command to view your current switch status policy configuration:

```
switchStatusPolicyShow
```

By setting the DOWN and MARGINAL value for a parameter to 0,0 that parameter is ignored in setting the overall status for the switch.

You must not change the settings unless directed to do so by EMC Technical Support.

Enabling the Track Changes Feature

To enable the track changes feature:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   ```
   trackChangesSet 1
   ```

   A prompt is displayed verifying that the track changes feature is on. The output from the track changes feature is dumped to the error log for the switch. Use the `errdump` command or `errshow` command to view the error log.

   Trackable changes are:

   - Successful login
   - Unsuccessful login
   - Logout
   - Config file change from task
   - Track changes on
   - Track changes off

   Items in the error log created from the track changes feature are labeled `Error TRACK`. For example:

```
switch:admin> errdump

Error 07
--------
0x17ef (fabos): Mar 24 11:10:27
Switch: 1, Info TRACK-CONFIG_CHANGE, 4, Config file change from
  task:TRACKIPC

Error 06
--------
0x4e7 (fabos): Mar 24 11:10:24
Switch: 1, Info TRACK-TRACK_ON, 4, Track-changes on
```

Displaying Whether Track Changes is Enabled

To display the status of the track changes feature:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `trackChangesShow`

   The status of the track changes feature is displayed as either `on` or `off`. This also displays whether the track changes feature is configured to send SNMP traps. For example:

```
switch:admin> trackchangesshow
Track changes status: ON
Track changes generate SNMP-TRAP: NO
```

Routing

In Order Delivery

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, some frames could be delivered out of order.

The default behavior is to automatically enable out-of-order delivery of frames during fabric topology changes; this enables fast rerouting after a fabric topology change. Refer to *Forcing In-Order Delivery of Frames* on page 2-19 to change the default routing settings during topology changes.

Dynamic Load Sharing

Routing is generally based on the incoming port and the destination domain. This means that all the traffic coming in from a port (either E_Port or Fx_Port) directed to the same remote domain is routed through the same output E_Port. To optimize fabric routing, when there are multiple equivalent paths to a remote switch, traffic is shared among all the paths. Load sharing is recomputed when a switch is booted up or every time a change in the fabric occurs. A change in the fabric is defined as an E_Port going up or down, or an Fx_Port going up or down. Refer to *Using Dynamic Load-Sharing* on page 2-19.

Configuring the In-Order Delivery Option

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, some frames may be delivered out of order.

The default behavior disables in-order delivery of frames during fabric topology changes. This enables fast rerouting after a fabric topology change.

Important Do not enable In-Order Delivery unless told to do so by EMC Technical Support.

Forcing In-Order Delivery of Frames

To force in-order delivery of frames during fabric topology changes:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
iodset
```

Important This command can cause a delay in the establishment of a new path when a topology change occurs, and should be used with care.

Disabling In-Order Delivery of Frames

To display in-order delivery of frames:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
iodreset
```

Using Dynamic Load-Sharing

Optimal load sharing is rarely achieved with DLS disabled. If DLS is turned on (using **dlsset**), routing changes can affect working ports. For example, if an Fx_Port goes down, another Fx_Port may be rerouted from one E_Port to a different E_Port. The switch minimizes the number of routing changes, but some are necessary in order to achieve optimal load sharing.

If DLS is turned off (using **dlsreset**), load sharing is performed only at boot time or when an Fx_Port comes up.

1. Log in to the switch as admin.
2. Enter the **dlsshow** command to view the current DLS setting.

   One of the following messages appears:

   - **DLS is set** The DLS option is turned on. Load sharing is reconfigured with every change in the fabric.
   - **DLS is not set** The DLS option is turned off. Load sharing is only reconfigured when the switch is rebooted or an Fx_Port comes up.
3. Enter the **dlsSet** command to enable Dynamic Load Sharing when a fabric change occurs.
4. Enter the dlsReset command to disable Dynamic Load Sharing.

   Load sharing is performed only at boot time or when an Fx_Port comes up.

Example:

```
switch:admin> dlsshow
DLS is not set
switch:admin> dlsset
Committing configuration...done.
switch:admin> dlsshow
DLS is set
switch:admin> dlsreset
Committing configuration...done.
```

Viewing Routing Path Information

1. Log in as admin.
2. Enter the **topologyShow** command to display the fabric topology, as it appears to the local switch.

   The following entries appear:

   - Local Domain — Domain number of local switch.
   - Domain — Domain number of destination switch.
   - Metric — Cost of reaching destination domain.
   - Name — The name of the destination switch.
   - Path Count — The number of currently active paths to the destination domain.

- Hops — The maximum number of hops to reach destination domain.
- Out Port — The Port that incoming frame will be forwarded to, in order to reach the destination domain.
- In Ports — Input ports that use the corresponding Out Port to reach the destination domain. This is the same information provided by **portrouteshow** and **urouteshow**.
- Total Bandwidth — The maximum bandwidth of the out port.
- Bandwidth Demand — The maximum bandwidth demand by the in ports.
- Flags — Always 'D', indicating a dynamic path. A dynamic path is discovered automatically by the FSPF path selection protocol.

Example:

```
switch:admin> topologyshow
2 domains in the fabric; Local Domain ID: 1
Domain: 6
Metric: 500
Name: switch
Path Count: 4
Hops: 1
Out Port: 60
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
Hops: 1
Out Port: 61
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
Hops: 1
Out Port: 62
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
Hops: 1
Out Port: 58
In Ports: None
Total Bandwidth: 2 Gbps
Bandwidth Demand: 0 %
Flags: D
```

1. Enter the **urouteshow** [*slotnumber*/][*portnumber*][, *domainnumber*] command to display unicast routing information.

   The following entries appear:

   - Local Domain — Domain number of local switch.
   - In Ports — Port from which a frame is received.
   - Domain — Destination domain of incoming frame.
   - Out Port — The Port that incoming frame will be forwarded to, in order to reach the destination domain.
   - Metric — Cost of reaching destination domain.
   - Hops — The maximum number of hops to reach destination domain.

- Flags — Indicates if route is dynamic (D) or static (S). A dynamic route is discovered automatically by the FSPF path selection protocol. A static route is assigned using the command **urouteconfig**.
- Next (Dom, Port) — Domain and port number of the next hop. These are the domain number and the port.

The example below displays the routing information of all the active ports:

:

```
switch:admin> urouteshow
Local Domain ID: 3
In Port Domain Out Port Metric Hops Flags Next (Dom, Port)
------------------------------------------------------------------------
0 1 11 1000 1 D 1,0
11 2 0 1500 2 D 4,0
4 0 500 1 D 4,0
16 1 27 1000 1 D 1,1
27 2 16 1500 2 D 4,16
4 0 500 1 D 4,0
```

The example below displays the routing information for port 11 on slot 1.

```
switch:admin> urouteshow 1/11
Local Domain ID: 3
In Port Domain Out Port Metric Hops Flags Next (Dom, Port)
------------------------------------------------------------------------
   -
11 2 16 1500 2 D 4,16
4 16 500 1 D 4,16
```

The example below displays the routing information of port 11 to domain 4 only:

```
switch:admin> urouteshow 1/11, 4
Local Domain ID: 3
In Port Domain Out Port Metric Hops Flags Next (Dom, Port)
------------------------------------------------------------------------
   -
11 4 16 500 1 D 4,16
```

Displaying Help Information for a Telnet Command

To display help information about a Telnet command:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   help ***command***

   where *command* is the command name you would like help with.

Reading Hexadecimal Port Diagrams

Many of the commands return port diagrams in hexadecimal format.

Example

```
switch:admin> bcastShow

Group   Member Ports    Member ISL Ports        Static ISL Ports

-----------------------------------------------------------------
 256      0x00000428        0x00000428              0x00000000
          0x00008020        0x00000020              0x00000000
          0x00000001        0x00000000              0x00000000
switch:admin>
```

To read the hexadecimal port diagrams, they must be converted into binary notation. Each hexadecimal value represents four binary values. Each hexadecimal value is converted into a group of four binary values that represent four ports as follows:

Hex value = Binary value

0 = 0000

1 = 0001

2 = 0010

3 = 0011

4 = 0100

5 = 0101

6 = 0110

7 = 0111

8 = 1000

9 = 1001

A = 1010

B = 1011

C = 1100

D = 1101

E = 1110

F = 1111

Once the hexadecimal value is converted into a binary bitmap, each bit represents a port, where a value of 1 means yes and a value of 0 means no. The bitmap is read from right to left; that is, the least significant bit represents port 0.

For example, if the member port value is displayed in hex as:

```
0     0     0   1     2  0     8     3

0000  0000  0000  0001  0010  0000  1000  0011
```

This bitmap displays the member ports as port 0, 1, 7, 13, and 16. Each switch has a hidden internal port (in the example above, port 16) that is always a member of a broadcast group.

3 Standard Security in Fabric OS

This chapter provides information regarding security features that are standard in the Fabric OS. Refer to the *Secure Fabric OS User's Guide* for information about licensed security features.

The following standard fabric security information is provided:

Overview

Some Security features are not supported. Refer to the Fabric OS release notes.

The following standard security information is specific to v4.1.0 firmware.

Standard security in FOS depends on account and password management. The information in this chapter discusses security that is available without Secure Fabric OS. For information regarding Secure Fabric OS, refer to the *Secure Fabric OS User's Guide*.

New Features

Ensuring a Secure Operating System

Fabric OS v4.1.0 uses Linux as the operating system in the switch. Therefore, securing the switch includes securing the underlying operating system as well.

Fabric OS uses the Berkeley r-commands facility to transfer data between control processors in the ED-12000B platform. The primary security concern is the use of the `.rhosts` file. All hosts listed in the.rhosts file are trusted, meaning they can log in to the switch without any authentication such as a password. The `.rhosts` file on the switch contains the IP address 10.0.0.5 and 10.0.0.6, which are the IP address of each CP in a ED-12000B chassis. To prevent the use of these facilities except from the internal network, an iptables firewall has been implemented. This firewall isolates the external network from internal network and does not allow execution of r-commands on the switch from external hosts. However, if you logged in to a switch of CP as root, you can issue r-commands to the other CP.

In addition, various proprietary protocols are also used over the internal CP-to-CP Ethernet. The internal Ethernet interface is considered a "trusted" interface over which arbitrary communications may occur. To address these security concerns, the internal Ethernet interfaces were disconnected from the public Ethernet interfaces.

A packet filter is used to isolate the internal Ethernet interface. The packet filter:

- Prevents routing of packets to and from internal network.
- Protects against spoofing of internal network addresses.
- The packet filter blocks all incoming packets from 10.0.0.0 to 10.0.0.255.
- Closes network services intended only for the internal network without changing the source code.

Firewalling with iptables

The Linux kernel contains advanced tools for packet filtering — the process of controlling network packets as they attempt to enter, move through, and exit your system. Iptables are similar to ipchains (which were available in pre-2.4 kernels) but greatly expands on the scope and control available for filtering network packets.

For more information about configuring iptables, refer to the Redhat website:

```
http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/
   ref-guide/ch-iptables.html
```

About Secure Shell (SSH)

An SSH (Secure Shell) is used to support encrypted telnet sessions to the switch (DES encryption is not supported). The default out-of-band Telnet mechanism for managing switches was deemed insecure because the passwords are sent over the wire in clear text. It is relatively easy for any network-connected system to sniff and reap these passwords for use in subsequent intrusions. In a complex enterprise network that aggregates device management into a backbone, it is difficult to prevent, or even detect, these attempts to sniff passwords. Secure Shell (SSH), is an alternative to Telnet, and uses strong encryption to prevent password sniffing and enhance the privacy of the management link.

SSH encrypts all messages, including the client sending the password at login time. This is a significant improvement over the basic **telnet** and **sectelnet**, which encrypts only the login password. The SSH package contains a daemon (sshd) which runs on the switch, and is very similar to **telnetd**, except that all messages are encrypted. The SSH daemon supports a wide variety of encryption algorithms, such as Blowfish-CBC, AES, etc.

The daemon requires keys (public/private) for encryption. These keys are generated by a program called **ssh-keygen** when the **openssh** RPM is installed. The keys are saved to files in `/etc directory` and sshd will read them on startup:

ssh_host_dsa_key
ssh_host_dsa_key.pub
ssh_host_rsa_key
ssh_host_rsa_key.pub
ssh, config --> configuration file sshd server

Supported versions and features:

- Officially support version 2 of the SSH protocol. (ssh2). ssh2 uses DSA key for authentication. The DSA authentication key is 1024 bits.
- The daemon will run under root identity.
- A user cannot save their public keys on the switch. A password is the only method of authentication.

- The following default ciphers for session encryption are supported: AES128-CBC, 3DES-CBC, Blowfish-CBC, Cast128-CBC, and RC4.
- The following HMACs are supported: HMAC-MD5, HMAC-SHA1, HMAC-SHA1-96, HMAC-MD5-96.

If you telnet to another machine, and then start a SSH session inside that telnet session, the telnet traffic is still in clear text and not secure.

The FTP protocol is not secure. When you FTP to or from the switch, the contents are in clear text. This includes the remote FTP server's login and password. This limitation affects the following commands: **savecore**, **configupload**, **configdownload**, and **firmwaredownload**.

SSH Server is installed automatically with the v4.1.0 firmware download and reboot of the switch. No further action is required for the SSH Server. However, the SSH Client will still need to be installed (refer to *Installing and Configuring a Secure Shell (SSH) Client*).

Installing and Configuring a Secure Shell (SSH) Client

The SSH Server is installed automatically with v4.1.0; use the information below to select and install the SSH Client.

The SSH Client must support v2 of the SSH protocol.

Below are three options for installing the SSH Client:

EMC does not support or recommend any specific SSH Client applications.

Two well known SSH Clients that have been tested are PuTTY and F-Secure.

- **PuTTY**:
  Putty is an SSH1+SSH2 implementation; it is a free implementation of Telnet and SSH for Win32 platforms.
- **F-Secure**:
  F-Secure also provides a SSH protocol that support v1 and v2. The docs are available for free from the f-secure.com web site.
- **openssh.com**:
  Openssh may also provide an appropriate SSH Client. However, any SSH Client that you choose must support v2 of the SSH Protocol.

Refer to the following for installation suggestions:

- *Installing and Configuring PuTTY*, which follows

  or

- *Installing and Configuring F-Secure SSH* on page 3-11

Installing and Configuring PuTTY

1. Download PuTTY from the following web site:

   www.openssh.com/windows.html

2. Click the PuTTY icon on your desktop after installation is complete.

The PuTTY Configuration appears, as displayed in Figure 3-1:

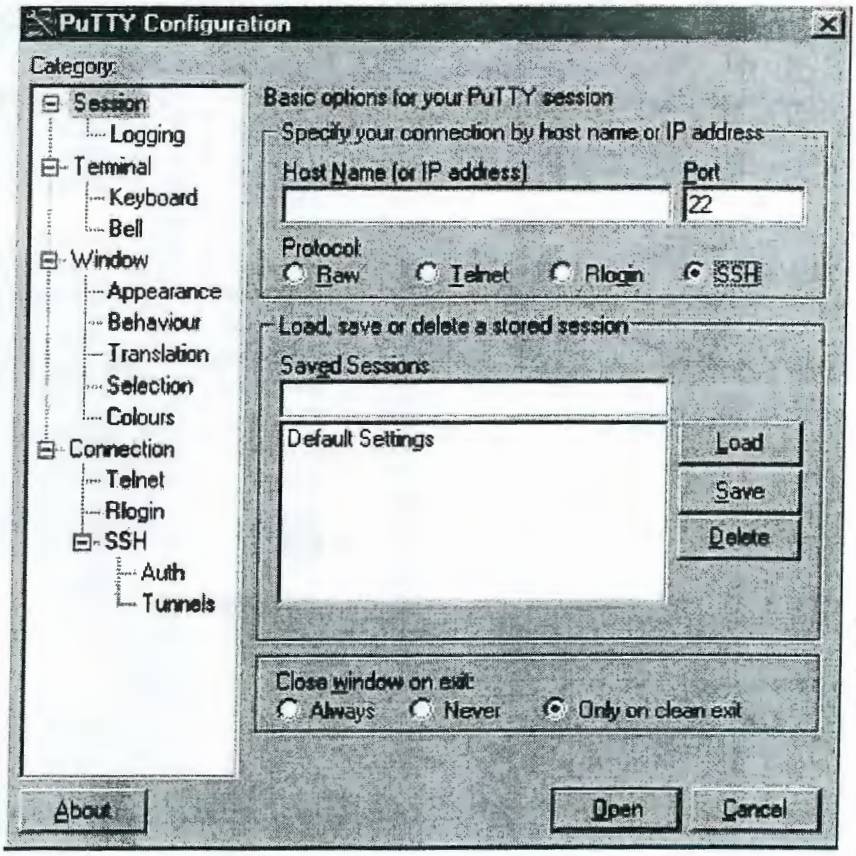


Figure 3-1 PuTTY Configuration Window

3. Select Session from the Category column (located on the left).
4. Locate the Host Name field. Enter the IP address of the switch that you want to connect to via SSH.

   SSH uses port 22 by default.

If your site is using a firewall, the Port field is where you would change the port number. Please contact your system administrator for more information.

---

5. Locate the Saved Sessions field. Enter a session name and then click the Save button; keep the session name for future reference.

6. Select SSH from the Category column (located on the left).

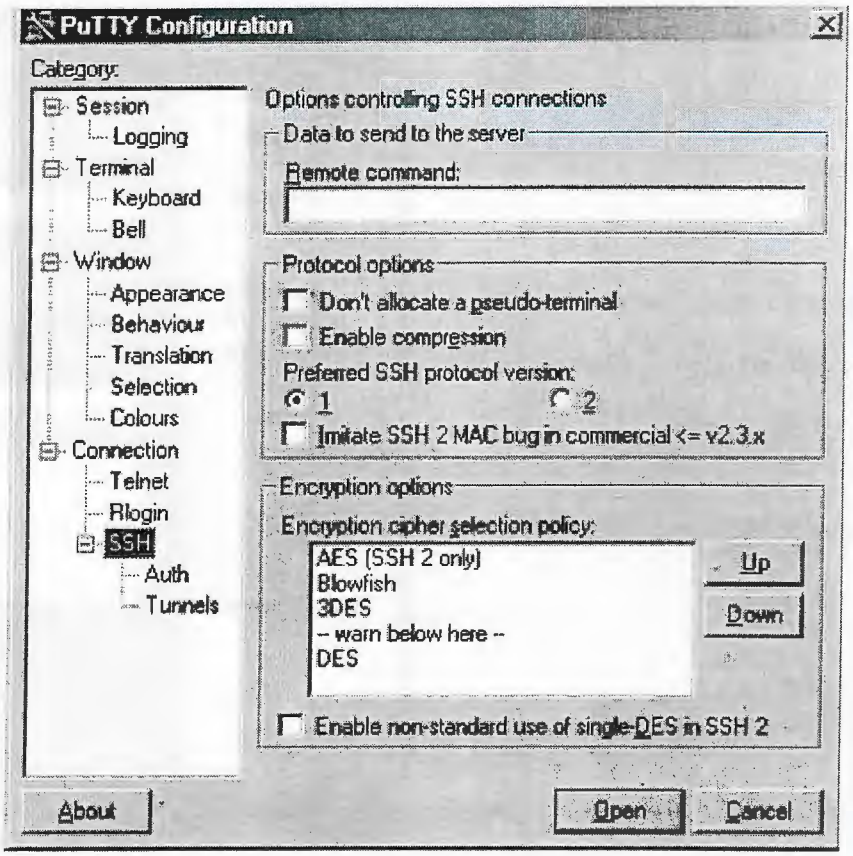


Figure 3-2 PuTTY Configuration - SSH Options

7. Locate Protocol Options - *Preferred SSH protocol version*. Select the 2 radio button.
8. Click the Auth selection from the Category column (located under SSH).
9. Check the Attempt "keyboard-interactive" Authentication (SSH2) box.

10. Click the Tunnels selection from the Category tree (tunnels is nested under SSH).

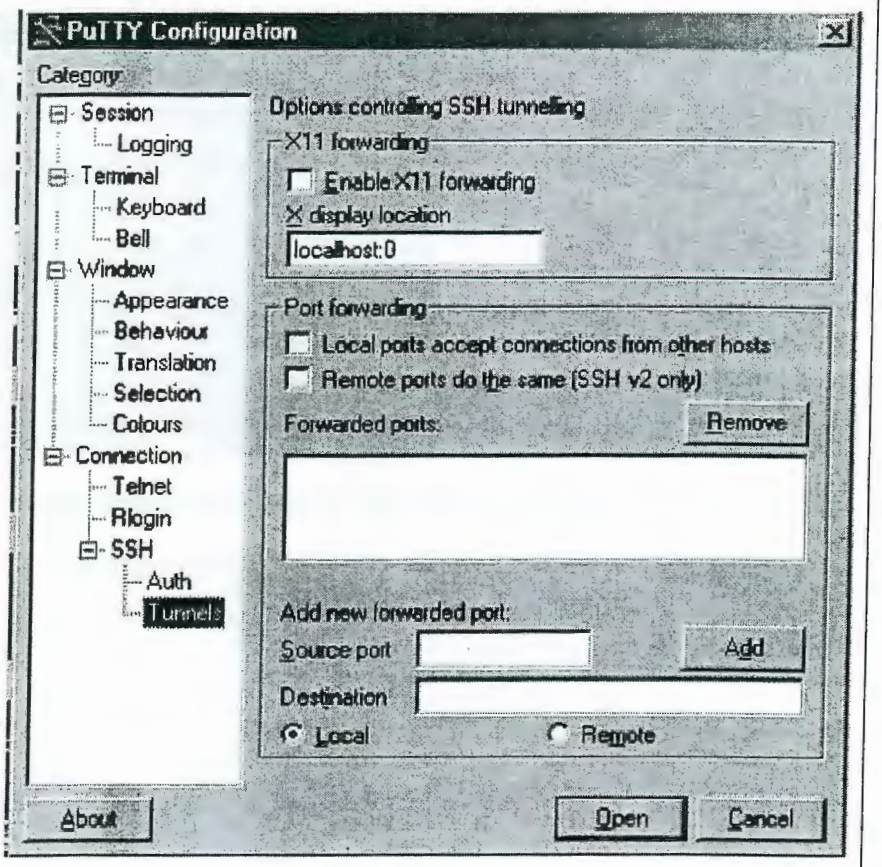


Figure 3-3 PuTTY Configuration - Tunnel Options

11. Enter a local host number in the *X display location* field.
12. Select the *Local* radio button.
13. Select the Open button.

The PuTTY Security Alert dialog box appears the first time you connect.

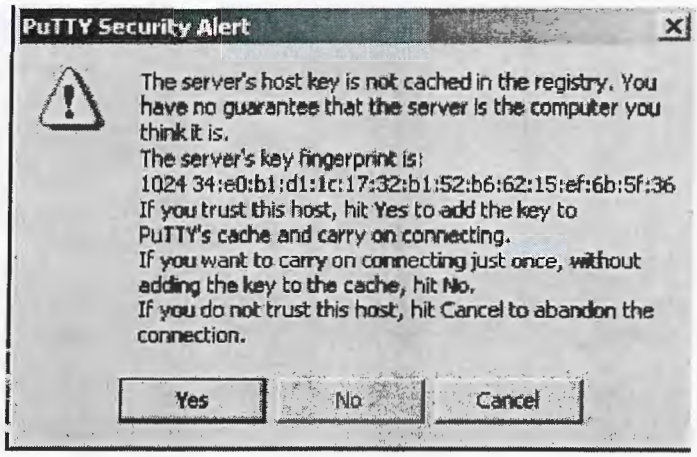


Figure 3-4 **PuTTy Initial Connection Security Alert**

Troubleshooting PuTTY

PuTTY provides optional logging, which can be useful for troubleshooting.

1. Select Logging from the Category tree (logging is nested beneath Session in the Category tree).

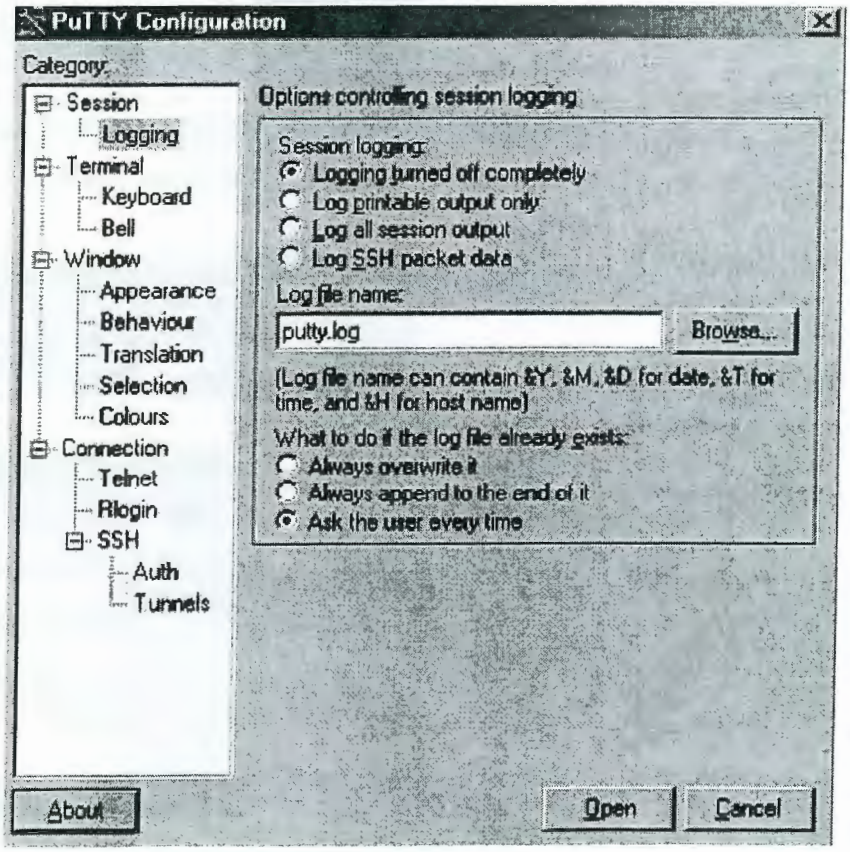


Figure 3-5 PuTTY Logging Window

2. Configure Logging as appropriate.

   The User Name and Password appear in the log by default when Logging is enabled. This is expected behavior; for security purposes, use caution when enabling logging.

Installing and Configuring F-Secure SSH

A 30-day free trial is available from F-Secure.com.

1. Download the SSH Client from f-secure.com.

   You can also download free documentation.

2. Click on the SSH Client icon to invoke the F-Secure Client:

The F-Secure SSH Client Default Window appears.

3. Click the Quick Connect button to open the Client Startup window.

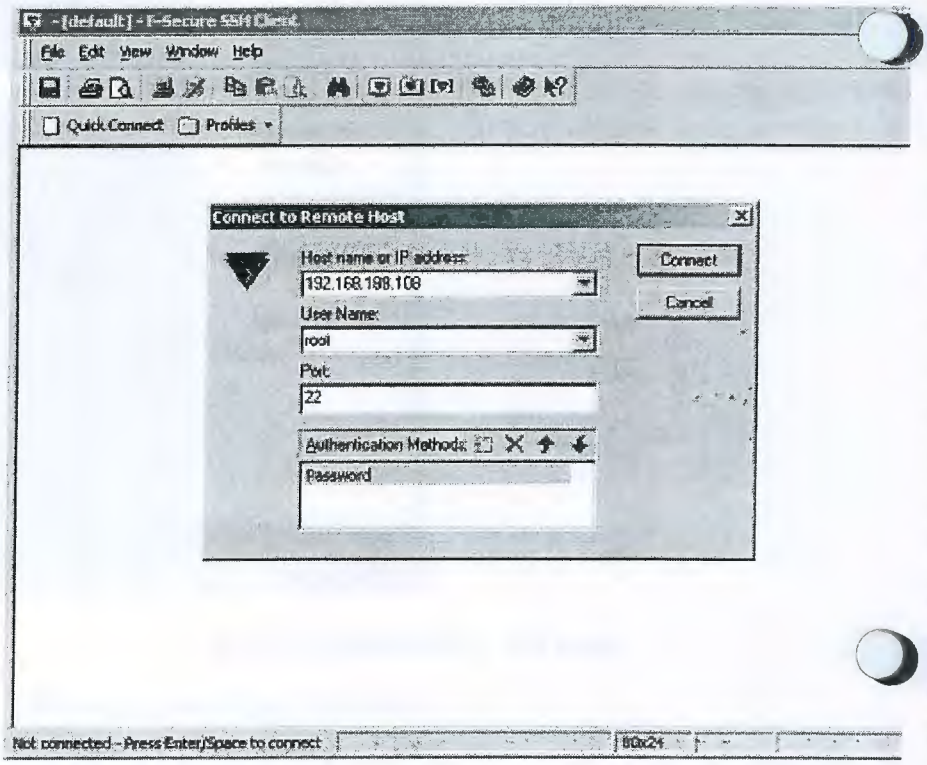


Figure 3-6 F-Secure SSH Client Startup Window

4. Enter the Host IP address, User Name, and Authentication information.

   Port 22 is used by SSH by default.

5. Click Connect.

   The Host Identification dialog box appears.

6. (Optional) Save the new Host Key to a local database. Select Yes or No.

   The Password dialog box appears.

7. Enter a password.

   Disclaimer information appears, and a session is started.

Troubleshooting the F-Secure SSH Client

Contacting Technical Support

In the event of a malfunction or bug in the program, a dialog box appears.

1. Select **Help** > **Troubleshooting**.
2. Select the Copy to Clipboard button to save any relevant information about the problem.
3. Go to `http:/www.f-secure.com/support`.

Additional SSH Resources

- *SSH, The Secure Shell; The Definitive Guide.* By O'Reilly.
- SSH IETF website:

  `http://www.ietf.org/ids.by.wg/secsh.html`

Disabling the Telnet Interface

From a security standpoint, with the addition of SSH, the telnet interface is no longer necessary to manage the switch. Some customers may wish to disable telnet to prevent a user from passing cleartext passwords over the network when logging in to the switch. The **configure [telnetd]** command is provided to allow customers to disable the telnet interface. The default configuration of the switch will ship with telnet enabled.

For more information on the **configure** command, refer to the *Fabric OS Reference Guide.*

1. Log in to the switch as admin.
2. Enter **configure [telnetd]** at the command line.

   This configure command can be run with the switch enabled.

3. Press <enter>.

   The Telnet interface is disabled.

   SNMP, HTTP, API, RSNMP, WSNMP, SES, and MS are managed through their respective policies when security is enabled. Refer to the *Secure Fabric OS User's Guide* for information.

Listeners

In order to make the Fabric OS more secure, the principal has been adopted that the Linux subsystem should provide only the minimal necessary functionality required to implement supported features and capabilities.

Removal of Unused Listeners

Changing the principal to provide the minimum Linux subsystem functionality required that a number of listeners be removed from this version of the Fabric OS.

Some listeners are required for CP to CP communications on the internal network of the ED-12000B. These listeners are blocked on the ED-12000B, and are not started on the DS-32B2.

Table 3-2 Removed Listeners for the ED-12000B and DS-32B2

Listener Name	ED-12000B	DS-32B2
chargen	Do not start	Do not start
echo	Do not start	Do not start
daytime	Do not start	Do not start
discard	Do not start	Do not start
ftp	Do not start	Do not start
rexec	Block with packet filter	Do not start
rsh	Block with packet filter	Do not start
rlogin	Block with packet filter	Do not start
time	Block with packet filter	Do not start
rstats	Do not start	Do not start
rusers	Do not start	Do not start

Passwords

About Passwords

There are four accounts for each switch instance. For a ED-12000B, there are four accounts for switch instance 0, and four accounts for switch instance 1. The account names are the same for the both switch instances. For the DS-32B2, there are four accounts. Refer to Table 3-3 and Table 3-4.

All account names remain to be the same as Fabric OS v4.0: *root, factory, admin,* and *user.*

At each account level, you can change passwords for that account and all accounts that have lesser privileges.

There is one exception to the password structure; an admin level user can change the root password by entering the **passwd** "root". They must also know the old root password.

Password Levels

There are four levels of account access:

- root — not recommended
- factory — not recommended
- admin — recommended for administrative operations
- user — recommended for non-administrative operations

Therefore, if you are logged in as admin, you can change the passwords for both admin and user (see noted exception).

Table 3-3 DS-32B2 Password Accounts

One logical Switch	root	one password	
	factory	one password	
	admin	one password	
	user	one password	

The ED-12000B switch has two logical switches, each logical switch has its own set of four passwords.

Table 3-4 12000 Switch - Password Accounts

Single ED-12000B Switch			
Logical Switch 0	root	one password	**One Set of Passwords**
	factory	one password	
	user	one password	
	admin	one password	
CPs			**One Set of Password**
Logical Switch 1	root	one password	**One Set of Passwords**
	factory	one password	
	user	one password	
	admin	one password	

Record your passwords and store in a secure place, as recovering passwords may require significant effort.

Default Fabric and Switch Accessibility

Hosts:

- Any host can access the fabric by SNMP
- Any host can telnet to any switch in the fabric
- Any host can establish an HTTP connection to any switch in the fabric
- Any host can establish an API connection to any switch in the fabric

Devices:

- All device ports can access SES

- All devices can access the management server
- Any device can connect to any FC port in the fabric

Switch Access:

- Any switch can join the fabric
- All switches in the fabric can be accessed through serial port
- All switches in the fabric that have front panels (some of the 2000 series) can be accessed through the front panel

Zoning:

- Node WWNs can be used for WWN-based zoning

Comparing Password Behavior Between Firmware Versions

The following tables provides detailed password information for v2.6/3.0, v2.6.1/3.1, v4.0 and v.41:

- *Account/Password Characteristics Matrix*
- *Password Prompting Matrix*
- *Password Recovery Options*
- *Password Migration Behavior During Firmware Upgrade/Downgrade*

Password Management Information

The following Account/Password Matrix describes the password standards and behaviors between v2.6/3.0, v2.6.1/3.1, v4.0 and v.41.

Table 3-5 Account/Password Characteristics Matrix

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
How many accounts are on the switch?	4	4	4, chassis based	**ED-12000B** - 8, 4 per switch **DS-32B2** - 4
What are the various account login names?	root, factory, admin, user	root, factory, admin, user	root, factory, admin, user	root, factory, admin, user.
Can account names be changed? (Does the **passwd** command prompt for account name changes?)	Yes, when Secure FabOS is disabled; No, when Secure FabOS is enabled.	Yes, when Secure FabOS is disabled; No, when Secure FabOS is enabled.	No	No, regardless of security mode.

Table 3-5 Account/Password Characteristics Matrix

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
What is the maximum and minimum amount of characters for a password?	Passwords can be minimum 8 chars and maximum 40 characters with printable ASCII	Passwords can be minimum 8 chars and maximum 40 characters with printable ASCII	0 - 8 (Standard UNIX)	Passwords can be minimum 8 chars and maximum 40 characters with printable ASCII
Can different switch instances use a different password for the same account login level? For example, the password for admin0 can be different from password for admin1.	N/A	N/A	No	Yes for ED-12000B switch. No for DS-32B2.
Does the root account use restricted shell?	No	No	No	No
When logging in to a factory installed switch, do you use the default passwords?	Yes	Yes	Yes	Yes

Table 3-5 Account/Password Characteristics Matrix

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
Does a user need to know the old passwords when changing passwords by the "**passwd**" command?	Yes, the old password is required to change any password, regardless of the level at which they login.	Yes, the old password is required to change any password, regardless of the level at which they login.	Yes, except when "root" is changes someone else's password. This is standard UNIX behavior; no additional security is enforced.	Old password is required only when changing password for the same level user password. Changing password for lower level user doesn't require old password. For example, users login as admin; old admin password is required to change the admin password. But old user password is not required to change the user password.
Can "**passwd**" change higher-level passwords? For example, can admin change root password?	No. If users login as admin, the users can only change admin and user passwords; the users cannot change factory, nor root password.	No. If users login as admin, the users can only change admin and user passwords; the users cannot change factory, nor root password.	Yes, but will ask for the "old password" of the higher-level account (example "root").	Yes; if users login as admin, they can change the root, factory, and admin passwords. However, if one logs in as user, one can only change the user password.

Table 3-5 Account/Password Characteristics Matrix

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
Can API change passwords?	API can change admin passwords on any switch, when security mode is disabled. It can only change the admin password on the Primary FCS switch when security mode is enabled.	API can change admin passwords on any switch, when security mode is disabled. It can only change the admin password on the Primary FCS switch when security mode is enabled.	Yes, only for admin.	Yes, only for admin.
Can WebTools change passwords?	When security mode is disabled, users can change the admin and user passwords on all switches using WebTools. When security mode enabled, users can only change the admin and user passwords on the Primary FCS switch using WebTools.	When security mode is disabled, users can change the admin and user passwords on all switches using WebTools. When security mode enabled, users can only change the admin and user passwords on the Primary FCS switch using WebTools.	No	No
Can SNMP change passwords?	No	No	No	No

Password Prompting Behaviors

The following table describes the expected password prompting behaviors between v2.6/3.0, v2.6.1/3.1, v4.0 and v.41.

Table 3-6 Password Prompting Matrix

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
Must *all* password prompts be completed for *any* change to take effect?	Yes. If users only provide some of the passwords before exiting, no passwords will be changed. Prompting will continue on the next appropriate login.	Yes. If users only provide some of the passwords before exiting, no passwords will be changed. Prompting will continue on the next appropriate login.	No. Partial changes of all four passwords are allowed.	No. Partial changes of all four passwords are allowed.
When does the password prompt appear?	When users login as root, factory, or admin.	When users login as root, factory, or admin.	When users login as root, factory, or admin, the accounts with default password will be prompted for change. The accounts with non-default password will NOT be prompted.	When users login as root, factory, or admin, the accounts with default password will be prompted for change. The accounts with non-default password will NOT be prompted.
Is a user forced to answer password prompts before getting access to the firmware?	No, users can type in CTRL-C to get out of password prompting.	No, users can type in CTRL-C to get out of password prompting.	No, users can type in CTRL-C to get out of password prompting.	No, users can type in CTRL-C to get out of password prompting.
Do users need to know the old root password when answering prompting?	No	No	Yes in v4.0 *No in v4.0.2 only	No

Table 3-6 Password Prompting Matrix (*continued*)

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
Are new passwords forced to be set to something different than the old passwords?	Yes	Yes	Yes	Yes
Is password prompting disabled when security mode is enabled?	Yes	Yes	Yes	Yes
Is the "**passwd**" command disabled until the user has answered password prompting?	True	True	False	True
Does password prompting reappear when passwords are changed back to default using the "**passwd**" command?	No	No	Yes	Yes
Does password prompting reappear when passwords are changed back to default using the "**passwdDefault**" command?	Yes	Yes	Yes	Yes. Will also run in secure mode on any FCS switch.

Password Recovery Options

The following table describes the options available when one or more types of passwords are lost.

Table 3-7 Password Recovery Options

Topic	V2.6/3.0	V2.6.1/3.1	V4.0	V4.1.0
If all the passwords are forgotten, what is the password recovery mechanism? Are these procedures non-disruptive recovery procedures?	The user has to get a special password recovery firmware based on the WWN of the switch from Tech Support, and then download the special firmware; this resets all passwords to default.The procedures are disruptive.	The user has to get a special password recovery firmware based on the WWN of the switch from Tech Support, and then download the special firmware; this resets all passwords to default.The procedures are disruptive.	Contact EMC Technical Support. A non-disruptive procedure is available.	Contact EMC Technical Support. A non-disruptive procedure is available.
If a user has only the root password, what is the password recovery mechanism?	Option 1: Use "**passwd**" command to set other passwords. Option 2: Use "**passwdDefault**"command to set all passwords to default.	Option 1: Use "**passwd**" command to set other passwords. Option 2: Use "**passwdDefault**"command to set all passwords to default.	Root can change any password by using the "**passwd**" command.	Use **passwd** command to set other passwords.
How to recover boot PROM password?	N/A	N/A	N/A	Contact Technical Support. Refer to *About Boot Prom Passwords* to set the boot PROM and recovery passwords.
How do I recover a user, admin, or factory password?	Refer to *Recovering a User, Admin, or Factory Password.*	Refer to *Recovering a User, Admin, or Factory Password.*	Refer to *Recovering a User, Admin, or Factory Password.*	Refer to *Recovering a User, Admin, or Factory Password.*

Password Migration During Firmware Upgrade/Downgrade

The following table describes the expected outcome of password settings when upgrading or downgrading firmware for v2.6/3.0, v2.6.1/3.1, v4.0 and v.41.

Table 3-8 Password Migration Behavior During Firmware Upgrade/Downgrade

Topic	V2.6/3.0	V2.6.1/3.1	V4.0.x	V4.1.0
When upgrading to a newer firmware release for the first time, which passwords will be used?	For first time firmware upgrades from v2.4.x to v2.6.0x, the v2.4.x passwords will be preserved.	For first time firmware upgrades from v3.0.x to v3.1.0, the v3.0.x passwords will be preserved.	N/A	For first time firmware upgrades from v4.0.x to v4.1.0, the v4.0.x passwords will be preserved.
Which passwords will be preserved during subsequent firmware upgrades?	For second firmware upgrades (and each subsequent upgrade) from v2.4.x to v2.6.0x, the passwords that were last used in v2.6.0x would be effective.	For second firmware upgrades (and each subsequent upgrade) from v3.0.x to v3.1, the passwords that were last used in v3.1 would be effective.	N/A	For second firmware upgrades (and each subsequent upgrade) from v4.0.x to v4.1.0 the passwords that were last used in v4.0.x are effective.
Is downgrading to an older firmware version (which does not support Secure Fabric OS) allowed when security mode is enabled?	Yes. **FirmwareDownload** does not prevent such downgrades.	Yes	N/A	Yes

Table 3-8 Password Migration Behavior During Firmware Upgrade/Downgrade

Topic	V2.6/3.0	V2.6.1/3.1	V4.0.x	V4.1.0
Which passwords will be used if downgrading to an older firmware for the first time?	When downgrading firmware from v2.6.0x to v2.4.x for the first time, the default passwords are used.	When downgrading firmware from v3.1.0 to v3.0.x for the first time, the default passwords are used.	N/A	If the switch had v4.1.0 factory installed, a firmware downgrade from v4.1.0 to v4.0.x uses the default passwords.
When downgrading to an older firmware at subsequent times, which passwords will be used?	Firmware downgrades from v2.6 to v2.4 use the previous v2.4 passwords (the passwords used before the firmware had been upgraded to v2.6).	Firmware downgrades from v3.1 to v3.0 use the previous v3.0 passwords (the passwords used before the firmware had been upgraded to v3.1).	Firmware downgrades within 4.x use the old 4.0 passwords.	Firmware downgrades from v4.1.0 to v4.0.x use the previous v4.0.x passwords (the passwords used before the firmware had been upgraded to v4.1.0).
When downgrading then upgrading again, what passwords will be used?	When upgrading firmware for a second time, the old v2.6 or v3.1 passwords will be used (the passwords used before the firmware had been downgraded).	When upgrading firmware for a second time, the old v2.6 or v3.1 passwords will be used (the passwords used before the firmware had been downgraded).	When upgrading firmware for a second time, the old passwords will be used (the passwords used before the firmware had been downgraded).	When upgrading firmware for a second time, the old passwords will be used (the passwords used before the firmware had been downgraded).

Managing Passwords

Modifying a Password

There are four levels of account access. Refer to *About Passwords*. To bypass the password prompt without completing the prompts, press CTRL + C.

1. Create a CLI connection to the switch.
2. Log in using the account for which you want to change the password.

   At each account level, you can change passwords for that account and all accounts that have lesser privileges. Refer to *About Passwords*.
3. Enter the **passwd** command and enter the requested information at the prompts.

   You must enter the current password for the first account. Passwords do not have to contain upper/lower/non-alphanumeric characters.

   If you are using Secure Fabric OS, new passwords are saved and distributed to all the switches in the fabric.

Example

```
cp0 login: admin
Password:
sec51_switch0:admin> passwd
Changing password for admin
Enter old password:
Enter new password:
Re-type new password:
Changing password for user
Enter new password:
Re-type new password:
```

4. Repeat for all switches in the fabric.

You cannot change account login names in Standard or Secure Mode.

Setting Recovery Passwords

About Boot Prom Passwords

Fabric OS v4.1.0 provides the option of setting the Boot PROM and Recovery passwords. This option does not apply to Fabric OS v3.1.0 or v2.6.1.

The Boot PROM and Recovery passwords provide an additional layer of security beyond the Root password.

- Setting a Boot PROM password protects the boot prompt from unauthorized use.
- Setting a Recovery password turns on the password recovery option, which requires a user to contact EMC Technical Support before recovering a Root or Boot PROM password.

Setting both the Boot PROM and Recovery passwords on all switches running Fabric OS v4.1.0 is strongly recommended. Not setting either of these passwords can compromise fabric security.

Setting Both the Boot PROM and the Recovery Passwords (DS-32B2)

Setting the Boot PROM and Recovery passwords requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

1. Connect to the serial port interface as described in step 1 of *Setting the Boot PROM Password Only (DS-32B2)*.
2. Reboot the switch.
3. Press **ESC** within four seconds after the message "Press escape within 4 seconds..." displays.

   The following options are available:

   1. Start system.
   2. Recovery password.
   3. Enter command shell.
4. Enter "2" at the prompt to set the Recovery password.
   The following message displays: "Recovery password is NOT set. Please set it now."
5. Enter the Recovery password.
   The Recovery password must be between 8 and 40 alphanumeric characters. A random password that is 15 characters or longer is

recommended for higher security. The firmware only prompts for this password once. It is not necessary to remember the Recovery password.

The prompt for the Boot PROM password displays: "New password:".

6. Enter the Boot PROM password, then re-enter when prompted. Record this password for future use.

   The new passwords are automatically saved (**saveenv** command not required).

7. Reboot the switch.
   Traffic flow resumes when the switch finishes rebooting.

Setting Both the Boot PROM and Recovery Passwords (ED-12000B)

The Boot PROM and Recovery passwords must be set for each CP card on a ED-12000B switch.

1. Connect to the serial port interface on the standby CP card, as described in step 1 of *Setting the Boot PROM Password Only (DS-32B2)*.
2. Log in to the active CP card by serial or telnet and enter the **hadisable** command to prevent failover during the remaining steps.
3. Reboot the Standby CP card by pressing the yellow ejector buttons at top and bottom of the CP card, then pressing both ejector handles back towards the switch to lock the card back into the slot.
4. Press **ESC** within four seconds after the message "Press escape within 4 seconds..." displays.

   The following options are available:

   1. Start system.
   2. Recovery password.
   3. Enter command shell.

4. Enter "2" at the prompt to set the Recovery password.
   The following message displays: "Recovery password is NOT set. Please set it now."
5. Enter the Recovery password.
   The Recovery password must be between 8 and 40 alphanumeric characters. A random password that is 15 characters or longer is

recommended for higher security. The firmware only prompts for this password once. It is not necessary to record the Recovery password.

The following prompt displays: "New password:".

6. Enter the Boot PROM password, then re-enter when prompted. Record this password for future use.

   The new passwords are automatically saved (**saveenv** command not required).

7. Failover the active CP card by entering the **hafailover** command. Traffic flow through the active CP card resumes when the failover is complete.
8. Connect the serial cable to the serial port on the new standby CP card (previous active CP card).
9. Repeat step 2 through step 7 for the new standby CP card (each CP card has a separate Boot PROM password).
10. Log in to the active CP card by serial or telnet and enter the **haenable** command to restore high availability.

Setting the Boot PROM Password Only (DS-32B2)

The option of setting the Boot PROM password only is available on a DS-32B2 and ED-12000B, but is not recommended. Refer to *Setting Both the Boot PROM and the Recovery Passwords (DS-32B2)*.

Setting the Boot PROM password requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

---

1. Create a serial connection to the switch. If Secure Mode is enabled, connect to the Primary FCS switch. If the switch does not have a serial port, contact EMC Technical Support.
   a. Connect the serial cable to the serial port on the switch and to an RS-232 serial port on the workstation.

      If the serial port on the workstation is RJ-45 instead of RS-232, remove the adapter on the end of the serial cable and insert the exposed RJ-45 connector into the RJ-45 serial port on the workstation.

   b. Disable any serial communication programs running on the workstation.

c. Open a terminal emulator application (such as HyperTerminal on a PC, or TERM or Kermit in a Unix environment), and configure the application as follows:

- In a Windows 95, 98, 2000, or NT environment:

Parameter	Value
Bits per second:	9600
Databits:	8
Parity:	None
Stop bits:	1
Flow control:	None

- In a UNIX environment, enter the following string at the prompt:

```
tip /dev/ttyb -9600
```

2. Reboot the switch by entering the **reboot** command.
3. Press **ESC** within four seconds after the message "Press escape within 4 seconds..." displays.

   The following options are available:

   1. Start system.
   2. Recovery password.
   3. Enter command shell.
4. Enter "3" at the prompt to enter the command shell.
5. Enter **passwd** command at the prompt.

This command is specific to the Boot PROM password when entered from the boot interface.

---

6. Enter the Boot PROM password at the prompt, then re-enter when prompted.
   The password must be 8 alphanumeric characters (any additional characters are not recorded).
7. Record this password for future use.
8. Enter the **saveenv** command to save the new password.
9. Reboot the switch by entering the **reset** command.
   Traffic flow resumes when the switch finishes rebooting.

Setting the Boot PROM Password Only (ED-12000B)

The option of setting the Boot PROM password only is available on a DS-32B2 and ED-12000B, but is not recommended. Refer to *Setting Both the Boot PROM and Recovery Passwords (ED-12000B)*.

On the ED-12000B, the suggested procedure is to set the password on the Standby CP, then failover; then set the password on the previously Active (now Standby) CPto minimize disruption to fabric.

The Boot PROM and Recovery passwords must be set for each CP card on a ED-12000B switch.

Setting the Boot PROM password requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted.

---

1. Determine the active CP card by opening a telnet session to either CP card, logging in as Admin, and entering the **hashow** command.
2. Log in to the active CP card by serial or telnet and enter the **hadisable** command to prevent failover during the remaining steps.
3. Create a serial connection to the standby CP card as described in *Setting the Boot PROM Password Only (DS-32B2)*.
4. Reboot the standby CP card by pressing the yellow ejector buttons at top and bottom of the CP card, then pressing both ejector handles back towards the switch to lock the card back into the slot. This causes the card to reset.
5. Press **ESC** within four seconds after the message "Press escape within 4 seconds..." displays.

   The following options are available:

   1) Start system.
   2) Recovery password.
   3) Enter command shell.

6. Enter "3" at the prompt to enter the command shell.
7. Enter **passwd** command at the prompt.

This command is specific to the Boot PROM password when entered from the boot interface.

---

8. Enter the Boot PROM password at the prompt, then re-enter when prompted.
   The password must be 8 alphanumeric characters (any additional characters are not recorded).
9. Record this password for future use.
10. Enter the **saveenv** command to save the new password.
11. Reboot the standby CP card by entering the **reset** command.
12. Failover the active CP card by opening a telnet session to the Active CP card, logging in as Admin, and entering the **hafailover** command.
    Traffic resumes flowing through the newly active CP card once it has completed rebooting.
13. Connect the serial cable to the serial port on the new standby CP card (previous active CP card).
14. Repeat step 3 through step 11 for the new standby CP card (each CP card has a separate Boot PROM password).
15. Log in to the active CP card by serial or telnet and enter the **haenable** command to restore high availability.

About Forgotten Passwords

Passwords can be recovered as follows:

- If the User, Admin, or Factory passwords are lost, but the Root password is known, follow the steps described in *Recovering a User, Admin, or Factory Password*.
- If the Root or Boot PROM password is lost, contact EMC Technical Support.

Recovering a User, Admin, or Factory Password

The User, Admin, and Factory passwords can be recovered if the Root password is known. The following procedure applies to all switch types and Fabric OS versions.

1. Open a CLI connection (serial or telnet) to the switch. If the Secure Mode of the Secure Fabric OS feature is enabled, connect to the Primary FCS switch.
2. Log in as Root.
3. Enter the command corresponding to the type of password lost:
   - passwd user
   - passwd admin
   - passwd factory

4. Enter the requested information at the prompts.

Recovering a Forgotten Root or Boot PROM Password

To recover a lost Boot PROM password, contact EMC Technical Support.

Frequently Asked Questions

Q: How many characters can a password have?

A: Passwords can be a minimum of 8 characters and a maximum of 40 characters. The password must contain two of the following classes: upper and lower case letters, digits, and non-alphanumeric characters.

Q: Do new passwords have to be set to something different than the old password or the default password?

A: Yes

Q: Does the end-user have to know the old password when changing passwords using the passwd command?

A: The end-user is prompted to use the old password when the account is being changed or has the same or higher privilege than the login account. For example, if the login account is admin, the old admin password is required to change the admin password. But, the old user password is not required for the admin account to change the user account password except when it is initially changed.

Q: Can the passwd command change higher-level passwords? For example, can admin level change root level passwords?

A: Yes. If end-users login as admin, the end-user can change root, factory, and admin passwords. However, if you login as user you can only change the user password. To change a higher level account, it is necessary to provide the high-level account old password to change the old account password.

Q: Can Web Tools change passwords?

A: No

Q: Can SNMP change passwords?

A: No

Q: When is the end-user prompted to change the password?

A: When you first login as root, factory, or admin you will be prompted to change the password, if the password is still default. Accounts with non-default passwords will not be prompted.

Q: Do users need to know the old root password when answering prompting?

A: No

Q: Is the password prompting disabled when security mode is enabled?

A: Yes

4

Working With ED-12000B

This chapter provides information on working with the ED-12000B. For detailed information about the ED-12000B, refer to the *EMC Connectrix Enterprise Director Model ED-12000B Hardware Reference Manual*.

Selecting Ports for the ED-12000B

In previous versions of the Fabric OS (v.2x and v3.x), the primary method for identifying a port within the fabric was the `domain,port` combination. For example, to add port 1 on domain 5 to a zone:

```
switch:admin> zoneadd "bluezone", "5,1"
```

This method of selecting ports cannot be used in the ED-12000B because of its additional slots and high port count. It was replaced in Fabric OS v4.0 by two methods to specify a particular port: the slot/port method and the port area number method.

Slot/Port Method

In the ED-12000B, a new method of selecting ports is required. To select a specific port, you must identify both the slot number and port number with which you are working.

When specifying a particular slot and port for a command, the slot number operand must be followed by the slash (/) and then a value for the port number. For example, to enable port 4 on a switch blade in slot 2, you would specify the following:

```
portEnable 2/4
```

The ED-12000B has a total of 10 slots counted 1 to 10. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are switch cards. On each switch card, there are 16 ports counted from the bottom 0 to 15. A particular port must be represented by both slot number (1 through 10) and port number (0 through 15).

No spaces are allowed between the slot number, the slash (/), and the port number.

Port Area Number Method

Some commands, such as zoning commands, require you to specify ports using the area number method. In the Fabric OS v4.0, each port on a particular domain is given a unique area ID.

The ED-12000B chassis contains two logical switches. The area IDs for both logical 64-port switches range from 0 to 63. Logical switch 0 and 1 both have a port that is referenced with area ID 0.

An area ID for each port is unique inside each logical switch (that is, each assigned domain ID). These are two of the three parts of a 24-bit Fibre Channel address ID:

- 8-bit Domain ID
- 8-bit Area ID
- 8-bit Port ID

Use the `switchshow` command to display all ports on the current (logical) switch and their corresponding area IDs.

Determining Area ID

To determine the Area ID of a particular port:

1. Log in to the switch as the admin user.
2. Enter the `switchshow` command. This command displays all ports on the current (logical) switch and their corresponding Area IDs.

The following example shows an ED-12000B:

```
switch12k:admin> switchshow
switch:admin> switchshow
switchName:     switch
switchType:     10.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   5
switchId:       fffc05
switchWwn:      10:00:00:60:69:00:54:e9
switchBeacon:   OFF
blade7: Beacon: OFF
blade9: Beacon: OFF

Area Slot Port Gbic Speed State
=====================================
  0    7    0   --    N2   No_Module
  1    7    1   --    N2   No_Module
  2    7    2   --    N2   No_Module
  3    7    3   id    N2   Online     F-Port  10:00:00:00:c9:24:0d:b3
  4    7    4   id    N2   Online     E-Port  10:00:00:60:69:00:54:e8 "san94"
   (upstream)(Trunk master)
  5    7    5   id    N2   Online     E-Port  (Trunk port, master is Slot  7 Port 4)
  6    7    6   id    N2   Online     E-Port  (Trunk port, master is Slot  7 Port 4)
  7    7    7   id    N2   Online     E-Port  (Trunk port, master is Slot  7 Port 4)
  8    7    8   --    N2   No_Module
  9    7    9   --    N2   No_Module
 10    7   10   --    N2   No_Module
 11    7   11   id    N2   No_Light
 12    7   12   id    N2   No_Light
```

```
 13    7   13   id    N2   No_Light
 14    7   14   id    N2   No_Light
 15    7   15   --    N2   No_Module
 32    9    0   --    N2   No_Module
 33    9    1   --    N2   No_Module
 34    9    2   --    N2   No_Module
 35    9    3   --    N2   No_Module
 36    9    4   --    N2   No_Module
 37    9    5   --    N2   No_Module
 38    9    6   --    N2   No_Module
 39    9    7   --    N2   No_Module
 40    9    8   id    N2   Online    E-Port  (Trunk port, master is Slot  9 Port 10)
 41    9    9   id    N2   Online    E-Port  (Trunk port, master is Slot  9 Port 10)
 42    9   10   id    N2   Online    E-Port  10:00:00:60:69:50:08:d5 "sqad11"
   (downstream)(Trunk master)
 43    9   11   id    N2   Online    E-Port  (Trunk port, master is Slot  9 Port 10)
 44    9   12   --    N2   No_Module
 45    9   13   --    N2   No_Module
 46    9   14   id    N2   No_Light
 47    9   15   id    N1   Online    L-Port  2 public
switch:admin>
```

Disabling a Port Blade

To disable a port card:

1. Log in to the switch as the admin user.
2. Enter the `slotoff` command with the following syntax:

   `slotoff` *`slotnumber`*

   where *`slotnumber`* is the slot number of the port card you want to disable.

Example

```
switch:admin> slotoff 7
switch:admin>
```

Enabling a Port Blade

To enable a port card:

1. Log in to the switch as the admin user.
2. Enter the `sloton` command with the following syntax:

   `sloton` *`slotnumber`*

   where *`slotnumber`* is the slot number of the port card you want to enable.

Example

```
switch:admin> sloton 7
switch:admin>
```

Powering On a Port Blade

To power on a port card:

1. Log in to the switch as the admin user.
2. Enter the `slotpoweron` command with the following syntax:

   `slotpoweron` *`slotnumber`*

   where *`slotnumber`* is the slot number of the port card you want to power on.

Example

```
switch:admin> slotpoweron 7
Powering on slot 7
switch:admin>
```

Powering Off a Port Blade

To power off a port card:

Before powering off a port card, you must disable it using the `switchdisable` command.

1. Log in to the switch as the admin user.
2. Enter the `slotpoweroff` command with the following syntax:

   `slotpoweroff` *`slotnumber`*

   where *`slotnumber`* is the slot number of the port card you want to power off.

Example

```
switch:admin> slotpoweroff 7
fabric: Reconfiguration due to Offline(port 4)
fabric: Reconfiguring at Sun Mar 24 13:42:22 2002
```

Displaying the Status of All Slots in the Chassis

To display the status of slots in the chassis:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `slotShow`

   This command displays the current status of each slot in the system. The format of the display includes a header and four fields for each slot. The fields and their possible values are as follows:

Slot	Displays the physical slot number.
Care Type	Displays the blade type: ◆ SW BLADE The blade is a Switch. ◆ CP BLADE The blade is a Control Processor. ◆ UNKNOWN The blade is not present or its type is not recognized.
ID	Displays the hardware ID of the blade type.
Status	Displays the Status of the blade: ◆ VACANT — The slot is empty. ◆ INSERTED, NOT POWERED ON — The blade is present in the slot but is turned off. ◆ DIAG RUNNING POST1 — The blade is present, powered on, and running the post initialization power on self tests (POST). ◆ DIAG RUNNING POST2 — The blade is present, powered on, and running the POST. ◆ ENABLED — The blade is on and enabled. ◆ DISABLED — The blade is powered on but disabled. ◆ FAULTY — The blade is faulty because an error was detected. ◆ UNKNOWN — The blade is inserted but its state cannot be determined.

The following example displays the status of all of the slots in the chassis:

```
switch:admin> slotshow

Slot   Blade Type    ID    Status
-------------------------------
  1     UNKNOWN            VACANT
  2     SW BLADE     2     ENABLED
  3     UNKNOWN            VACANT
  4     SW BLADE     2     ENABLED
  5     CP BLADE     1     ENABLED
  6     CP BLADE     1     ENABLED
  7     SW BLADE     2     ENABLED
  8     UNKNOWN            VACANT
  9     SW BLADE     2     ENABLED
 10     UNKNOWN            VACANT

switch:admin>
```

Determining the Active and Standby CPs

The ED-12000B has two control processors: an Active and a Standby. When accessed directly through the telnet, each has a different Fabric OS command set. The Standby control processor has only a subset of the Active control processor commands.

Important Since either control processor can be Active or Standby, it is important to identify which mode they are in prior to issuing commands. The only way to know whether the control processor is Active or Standby is to issue the `hashow` command.

A customer may telnet into a control processor and issue the `hashow` command to learn the status of the control processor. The `hashow` command performs the following functions:

It displays the control processor's status, including:

- Local CP state (slot number and CP id)
- Remote CP state (slot number and CP id)
- High Availability Enabled/Disabled
- Heartbeat Up/Down

Example

```
switch1:admin> hashow
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby
HA Enabled, Heartbeat Up
switch1:admin>
```

Setting the Blade Beacon Mode

When beaconing mode is enabled, the port LEDs will flash amber in a running pattern from port 0 through port 15 and back again. The pattern continues until the user turns it off. This can be used to signal the user to a failing unit.

To set the blade beacon mode on:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `bladebeacon slotnumber, mode`

   where `slotnumber` is the blade where you want to enable beacon mode, and mode is `1` to turn on beaconing, and `0` to turn off beaconing.

Displaying Information on Switch FRUs

To view field replaceable unit (FRU) information for a switch:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

   `chassisShow`

   This command displays the field replaceable unit (FRU) header content for each object in the chassis. This command returns information for each FRU including:

   - Object ID and object number. Valid values include the following:
     - CHASSIS
     - FAN
     - POWER SUPPLY
     - SW BLADE (switch)
     - CP BLADE (control processor)
     - WWN
     - UNKNOWN

     The object number refers to the slot number for blades, and unit number for everything else.
   - FRU header version number
   - The object's power consumption
     - Positive for power supplies
     - Negative for consumers
   - Part number (up to 14 characters)
   - Serial number (up to 12 characters)
   - The date the FRU was manufactured
   - The date the FRU header was last updated
   - The cumulative time, in days, that the FRU has been powered on
   - The current time, in days, that the FRU has been powered on
   - The externally supplied ID (up to 10 characters)
   - The externally supplied part number (up to 20 characters)
   - The externally supplied serial number (up to 20 characters)
   - The externally supplied revision number (up to 4 characters)

Example

```
switch:admin> chassisshow

SW BLADE  Slot: 2
Header Version:          2
Power Consume Factor:    -200
Brocade Part Num:        10-9238367-12
Brocade Serial Num:      1013456800
Manufacture:             Day:  7  Month: 12  Year: 2000
Update:                  Day: 23  Month:  3  Year: 2002
Time Alive:              181 days
Time Awake:              3 days
ID:                      555-374757
Part Num:                234-294-12345
Serial Num:              27346589
Revision Num:            A.00

SW BLADE  Slot: 4
Header Version:          2
Power Consume Factor:    -200
Brocade Part Num:        10-9238367-12
Brocade Serial Num:      1013456800
Manufacture:             Day:  7  Month: 12  Year: 2000
Update:                  Day: 23  Month:  3  Year: 2002
Time Alive:              181 days
Time Awake:              3 days
ID:                      555-374757
Part Num:                234-294-12345
Serial Num:              27346589
Revision Num:            A.00

<output truncated>
```

5

Working With the Management Server

This chapter provides the following information about working with the Management Server platform database.

The Management Server allows a storage area network (SAN) management application to retrieve and administer the fabric and interconnect elements such as switches, servers, and storage devices. It is located at the fibre channel well-known address, FFFFFAh.

Management Server Platform service is available only with Fabric OS v2.3 and later. If the Management Server Platform service is started on a fabric that contains any switches with Fabric OS v2.2.x or earlier installed, the fabric segments.

Working With the Management Server

An Access Control List (ACL) of WWN addresses determines which systems have access to the Management Server database. These WWNs are usually associated with the management applications. Access to the Management Server is restricted to the WWNs listed in the ACL. If the list is empty (default), the Management Server is accessible to all systems connected in-band to the Fabric.

Displaying the Access Control List

To display the Management Server Access Control List (ACL):

1. Log in to the switch as the admin user.
2. Enter the `msconfigure` command. The command becomes interactive.
3. At the **Select** prompt, enter `1` to display the access list.

   A list of WWNs that have access to the Management Server displays.

Example

```
switch:admin> msconfigure

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [2] 1

MS Access List consists of (1): {
 20:01:00:60:69:00:60:01
}

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 0

done ...
switch:admin>
```

Adding a WWN to the Access Control List

To add a WWN to the ACL:

1. Log in to the switch as the admin user.
2. Enter the `msconfigure` command. The command becomes interactive.
3. At the **Select** prompt, enter `2` to add a member based on its Port/Node WWN.
4. At the **Port/Node WWN** prompt, enter the WWN of the member you would like to add to the ACL. Press the return key, and the main menu is displayed.
5. At the prompt enter `1` to verify the WWN you entered was added to the ACL.
6. Once you have verified that the WWN was added correctly, enter `0` at the prompt to end the session.
7. At the **Update the FLASH** prompt, enter `Y`.
8. Press ENTER to update the flash and end the session.

Example

```
switch:admin> msconfigure

0        Done
1        Display the access list
2        Add member based on its Port/Node WWN
3        Delete member based on its Port/Node WWN

select : (0..3) [1] 2

Port/Node WWN (in hex): [00:00:00:00:00:00:00:00]
   20:01:00:60:69:00:60:01
*WWN is successfully added to the MS ACL.

0        Done
1        Display the access list
2        Add member based on its Port/Node WWN
3        Delete member based on its Port/Node WWN

select : (0..3) [2] 1


MS Access List consists of (1): {
 20:01:00:60:69:00:60:01
}
0        Done
```

```
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN

select : (0..3) [1] 0

done ...
Update the FLASH?  (yes, y, no, n): [yes] y
*Successfully saved the MS ACL to the flash.

switch:admin>
```

Deleting a WWN From the Access Control List

To delete a WWN from the ACL:

1. Log in to the switch as the admin user.
2. Enter the msconfigure command. The command becomes interactive.
3. At the **Select** prompt enter `3` to delete a member based on its Port/Node WWN.
4. At the prompt, enter the WWN of the member you would like to delete from the ACL, then press ENTER. The main menu displays.
5. At the prompt, enter `1` to verify the WWN you entered was deleted from the ACL.
6. Once you have verified that the WWN was deleted correctly, enter `0` at the prompt to end the session.
7. Enter `Y` at the **Update the FLASH** prompt.
8. Press ENTER to update the flash and end the session.

Example

```
switch:admin> msconfigure

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 3

Port/Node WWN (in hex): [00:00:00:00:00:00:00:00]
   20:01:00:60:69:00:60:01
*WWN is successfully deleted from the MS ACL.

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [3] 1

MS Access list is empty
0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 0

done ...
```

```
Update the FLASH?  (yes, y, no, n): [yes] y
*Successfully saved the MS ACL to the flash.

switch:admin>
```

Displaying the Management Server Database

To view the contents of the Management Server Platform Database:

1. Log in to the switch as the admin user.
2. Enter the `msplatshow` command at the prompt. The contents of the Management Server Database display.

Example

```
switch:admin> msPlatShow
----------------------------------
Platform Name: [1] "c"
Platform Type: 9 : STORAGE_DEVICE
Number of Associated M.A.: 2
Associated Management Addresses:
[4] "snmp"
  [4] "http"
Number of Associated Node Names: 1
Associated Node Names:
  01:00:00:00:00:00:00:00

switch:admin>
```

Clearing the Management Server Database

To clear the Management Server Platform database:

1. Log in to the switch as the admin user.
2. Enter the `msplcleardb` command.
3. Enter `y` to confirm the deletion. The Platform database is cleared.

Example

```
switch:admin> msplcleardb

MS Platform Management Service is currently enabled.
This will erase Platform databases in the entire
   fabric.

Would you like to continue this operation? (yes, y, no,
   n): [no] y

Fabric-wide Platform DB Clear operation in
   progress.....

*[msPlClearDB]: Fabric-wise Platform DB Delete
   operation in progress...
done ...

switch:admin>
```

Displaying the Fabric Capability for Management Server

To display the capability of a fabric for Management Server support:

1. Log in to the switch as the admin user.
2. Enter the `mscapabilityshow` command. The name, WWN, and specific Management Server capability is displayed for each switch in the fabric.
3. Verify that each switch in the fabric is capable of Management Server support.

Example

```
switch:admin> msCapabilityShow

Platform
Switch WWN                Service Capable   Capability  Name
========================  ===============   ==========  =======
10:00:00:60:69:04:01:94         Yes         0x0000008f  "switch55"
10:00:00:60:69:10:53:48         Yes         0x0000000b  "switch53"
10:00:00:60:69:10:54:c8         Yes         0x0000000b  "switch52"
10:00:00:60:69:02:39:70         Yes         0x0000000b  "switch54"
10:00:00:60:69:20:10:52         Yes         0x0000000b  "switch43"
10:00:00:60:69:20:10:2b         No          0x00000009  "switch62"
10:00:00:60:69:10:53:3c         Yes         0x0000000b  "switch51"
10:00:00:60:69:04:11:17         Yes         0x0000008f  "switch57"

Capability Bit Definitions:
Bit 0: Basic Configuration Service Supported.
Bit 1: Platform Management Service Supported.
Bit 2: Topology Discovery Service Supported.
Bit 3: Unzoned Name Server Service Supported.
Bit 4: M.S. Fabric Zone Service Supported.
Bit 5: Fabric Lock Service Supported.
Bit 6: Timer Service Supported.
Bit 7: RSCN Small Payload Supported.
Others: Reserved.
WARNING! Platform Management Service CAN NOT BE activated for this
   Fabric!!!
Done.
switch:admin>
```

In the example above, the fabric does not support Platform Management Service because "switch62" is running Fabric OS v2.2.

ivating the Platform Management Service

To activate the Platform Management Service for a fabric:

1. Log in to the switch as the admin user.
2. Enter the `msplmgmtactivate` command.

Example

```
switch:admin> msplmgmtactivate

Activating Platform Management Service in the Fabric is
   in progress.....

*Completed activating Platform Management Service in
   the fabric!

switch:admin>
```

Deactivating the Platform Management Service

To deactivate the Platform Management Service for a fabric:

1. Log in to the switch as the admin user.
2. Enter the `msplmgmtdeactivate` command.
3. Enter `Y` to confirm the deactivation.

Example

```
switch:admin> msplmgmtdeactivate

MS Platform Management Service is currently enabled.

This will erase Platform configuration information
as well as Platform databases in the entire fabric.

Would you like to continue disabling? (yes, y, no, n):
   [no] y

Deactivating Platform Management Service is in
   progress......

*Completed deactivating Platform Management Service in
   the fabric!

switch:admin>
```

6

Diagnostics and Status

This chapter provides the following information on displaying port and switch status information:

Diagnostics

The purpose of the diagnostic subsystem is to evaluate the integrity of the system hardware. Diagnostics can be invoked in either of two ways:

- Manually (through the Fabric OS command line)
- During the power-on self test (POST)

During these test activities, the error messages generated are sent to the console, error logs, and possibly to non volatile storage. Each of these destinations may adjust the output format slightly to suit the purpose of the output media.

Manual Operation

During manual operation of diagnostics, the switch or blade typically needs to be in an offline state so as not to affect the fabric in which the switch is placed. There are exceptions to this policy. If a diagnostic needs the switch offline and finds the switch is active, it will not run, and exists without harm to the fabric.

Manual tests are useful in fault isolation and various stress test environments. There is no single test that will give a comprehensive indication of the hardware status. Tests must run in concert to achieve this goal.

Power-On Self Test (POST)

The POST gives a quick indication of hardware readiness when new hardware is brought into operation. These tests do not require user input to function, typically operate within a couple of minutes, and support minimal validation due to the restriction on test duration. Their purpose is to give a basic health check before new hardware is allowed to join a fabric.

These tests are divided into two groups: POST1 and POST2.

- POST1 validates the hardware interconnect of the switch/blade
- POST2 validates the ability of the switch/blade to pass data frames between the ports

Diagnostic Command Set

The diagnostic command set can be divided into two categories:

- Test Commands

  Test commands act on hardware and report anomalies when found.

- Control Commands

  Control commands act to support or evaluate the diagnostic operations independent of performing actual test of hardware circuitry.

Diagnostics can be manually run in two basic modes:

- Normal interactive mode
- Burnin mode

  Burnin mode has additional control commands for its operation.

Diagnostics can also be executed in:

- Power on self test (POST) operation

  In POST, diagnostics do not require user command input. They are automatically activated when FRUs are brought on line.

During all three modes of diagnostic operation, the same tests are executed. For example, the `spinSilk` command executed from the command line is the same SpinSilk executed in POST.

Many diagnostic commands require the switch or port card to be in an offline state. This ensures that the diagnostic test does not interfere with normal fabric traffic. If the switch or port card is not in an offline state, the diagnostic does not run and displays an error message.

The switch or port card can be taken offline by entering the `switchdisable` or the `bladedisable` command, respectively. For more information about these commands, refer to the *Fabric OS Reference Manual*.

The diagnostic commands can be used together to provide an overall picture of the health of the hardware or to isolate and validate the functionality. A series of tests have been structured to allow hardware validation and fault isolation: the `bladediag` and `bladediagshort` commands for the ED-12000B, and the `switchdiag` and `switchdiagshort` commands for the DS-32B2.

Diagnostic Test Commands

The following is a list of diagnostic test commands:

- portRegTest
- sramRetentionTest
- spinSilk
- spinFab
- crossPortTest
- portLoopbackTest
- backPort
- centralMemoryTest
- cmemRetentionTest
- cmiTest
- camTest
- turboramTest
- statsTest
- portLEDtest
- filterTest
- bladeDiag (port card diagnostic for the ED-12000B)
- bladeDiagShort (port card diagnostic for the ED-12000B)
- switchDiag (diagnostic for the DS-32B2)
- switchDiagShort (diagnostic for the DS-32B2)

Diagnostic Control Commands

The following is a list of diagnostic control commands:

- diagEnablePost
- diagDisablePost
- diagModeShow
- statsClear
- diagShow
- diagStatus
- diagReset
- diagCommandShow
- diagHelp
- forceError
- forcePortError

Persistent Error Log

This feature prevents messages of lesser severity from over-writing messages of greater severity. For example, *Warning* messages cannot over write *Error, Critical,* or *Panic* messages. The persistent error log has the following features:

- The error log sub-system supports persistent logging. Each switch has its own persistent log.
- The persistent log is preserved across power cycles and system reboots.
- The persistent log has a default capacity to store 1024 error log entries.
- The persistent log can be resized at run time without having to reboot the switch or the system.
- The persistent log can be resized at run time to configure a maximum of 2048 entries. The persistent log can be resized to anywhere between 1024 and 2048 entries.

The error log sub-system can save a maximum of 1536 messages in RAM, that is, a total of 256 messages for each error message level (Panic, Critical, Error, Warning, Info, and Debug). In addition, important messages are stored in a separate persistent error log to guarantee that they are not lost in case of power outage or system reboot.

- The persistent log is implemented as a circular buffer. When more than maximum entries are added to the persistent log, old entries are over-written by new entries.
- All error messages of levels Panic and Critical are automatically saved in the persistent log as they are logged. This guarantees that critical or panic level messages are not lost in the event of unexpected system reboot or fail-over.
- A new command to control and filter messages to be saved in the persistent error log is provided. For example, you can specify that all log messages of level *Warning* and more severe than *Warning* (basically *Error, Critical, Panic)* should be saved in the persistent error log.

- The commands `errdump` or `errshow` display a superset of the persistent log messages saved during previous system run time cycles and the error log messages generated during the current run time cycle.
- Options are provided to `errdump` command to display three options: all the errors (previous persistent log and the current run time log), only errors from the current run time cycle, or the errors from the persistent error log.
- Options are provided to clear the persistent error log (`errclear -p`).

Only the persistent error log can be resized. The run time error log cannot be resized.

Displaying the Error Log of a Switch

There are two ways to display the error log of a switch:

- Display the error log one page at a time
- Display the error log all at once

To display the switch error log one page at a time:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
ErrShow
```

To display the switch error log all at once:

1. Log in to the switch as the admin user.
2. At the command line, enter the following command:

```
ErrDump
```

Clearing the Switch Error Log

To clear the error log for a particular switch instance:

1. Log in to the switch as the admin user.
2. Enter the `errclear` command.

Example The following example shows how to clear the persistent error log on the Active CP of the ED-12000B or the DS-32B2.

```
switch:admin> errClear -p
switch:admin>
```

The following examples apply to the ED-12000B switch only.

Example The following example shows how to clear the current run time error log on the Standby CP, for the switch instance 0.

```
switch:admin> errClear -s 0
switch:admin>
```

Example The following example shows how to clear the persistent error log on the Standby CP, for the switch instance 0.

```
switch:admin> errClear -s 0 -p
switch:admin>
```

Setting the Error Save Level

To control the types of messages that are saved in the persistent error log:

1. Log in to the switch as the admin user.
2. Enter the `errsavelvlset` command at the prompt.

Example The following example shows how to enable saving of *Warning*, *Error*, *Critical*, and *Panic* messages in the persistent error log.

```
switch:admin> errSaveLvlSet 3
switch:admin>
```

The following example applies to the ED-12000B switch only.

Example The following example shows how to enable saving of *Warning*, *Error*, *Critical*, and *Panic* messages in the persistent error log on the Standby CP for the switch instance 0.

```
switch:admin> errSaveLvlSet -s 0 3
switch:admin>
```

Displaying the Current Error Save Level

To display the current value of the persistent error log save level for a given switch:

1. Log in to the switch as the admin user.
2. Enter the `errsavelvlshow` command at the prompt.

Example Following example shows how to display current error log save level.

```
switch:admin> errSaveLvlShow

Current message save level is = 3

switch:admin>
```

Resizing the Persistent Error Log

To resize the persistent error log:

1. Log in to the switch as the admin user.
2. Enter the `errnvlogsizeset` command at the prompt.

Example The following example shows how to resize the persistent error log to 1500 entries.

```
switch:admin> errNvLogSizeSet 1500

Persistent error log is resized to store 1500 entries

switch:admin>
```

The following example applies to the ED-12000B switch only.

Example The following example shows how to resize persistent log to save 1500 error log entries on the Standby CP, for switch instance 0. The value -s is added to save the 1500 log entries.

```
switch:admin> errNvLogSizeSet -s 0 1500

Persistent error log size is already 1500 entries

switch:admin>
```

Displaying the Current Persistent Error Log Configuration

To display the current maximum size of the persistent error log for a given switch:

1. Log in to the switch as the admin user.
2. Enter the `errnvlogsizeshow` command at the prompt.

Example The following example shows how to display persistent error log configuration.

```
switch:admin> errNvLogSizeShow
Persistent Error Log can store 1024 entries
```

The following example applies to the ED-12000B switch only.

Example The following example shows how to display persistent error log configuration on the Standby CP, for switch instance -0.

```
switch:admin> errNvLogSizeShow -s 0
Persistent Error Log can store 1024 entries
```

Configuring the Syslog Daemon

The Fabric OS can be configured to use a UNIX style syslog daemon (*syslogd*) process to read system events and forward system messages to users and/or write the events to log files on a remote UNIX host system.

syslogd Overview

The Fabric OS maintains an internal log of all error messages. The internal log buffers are limited in capacity; when the internal buffers are full, new messages overwrite old messages.

A switch can be configured to send error log messages to a UNIX host system that supports syslogd. This host system can be configured to receive error/event messages from the switch and store them in files on the computer hard drive. This enables the storage of switch error log messages on a host system and overcomes the size limitations of the internal log buffers on the switch.

The Syslogd is a process that runs on UNIX or LINUX systems that reads and logs messages to the system console, log files, other machines and users as specified by its configuration file. Refer to the manual pages and related documentation for your particular UNIX host system for more information on the *syslogd* process and its capabilities.

Note that the host system can be running UNIX, Linux or any other operating system as long as it supports standard *syslogd* functionality. The switch by itself does not assume any particular operating system to be running on the host system. The only requirement is that the host system must support standard *syslogd* to receive error log messages from the switch.

Error Message Format

Below is an example of an error/event message received by the remote syslogd host from the switch.

```
Jun 4 18:53:59 sqab186 kernel: 0x299 (fabos): Switch: 0, Info HAMKERNEL-IP_UP, 4,
   (session=16) Heartbeat up from Standby CP
```

The first two items are the event's date and time (as known by the UNIX host machine where syslogd is running) and the machine name that generated the message (In this case it is the name of switch). The word "kernel" is the name of the syslogd facility used by the switch to send error log messages to the remote host. The rest of the message is similar to the error log message output from the `errShow` command

line interface on the switch. The fields that are specific to the switch error log message are:

- ID of the task that generated the error (in the example this is **0x299**)
- Name of the task that generated the error (in the example this is **(fabos)**)
- Switch instance number (in the example this is **Switch 0**)
- Message severity level in word (in the example this is **Info**)
- The error message identifier consisting of the module name (in the example this is **HAMKERNEL**) and the message name (in the example this is **IP_UP**)
- Numeric value of the message severity level defined by the switch (in the example this is **4**)
- A descriptive text string (in the example this is Heartbeat up from Standby CP)

Message Classification

Syslogd messages are classified according to facility and priority (severity code). This enables a system administrator to take different actions depending on the error.

The Fabric OS supports 6 message severity levels for error log messages. The following table provides a mapping between severity levels used by the switch and the syslogd severity levels supported by the UNIX system.

Table 6-1 Severity Levels

Message severity Levels/Numerical Value	UNIX syslogd message severity levels/Numerical Value
Panic (0)	Emergency (LOG_EMERG) (0)
Critical (1)	Alert (LOG_ALERT) (1)
Error (2)	Error (LOG_ERR) (3)
Warning (3)	Warning (LOG_WARNING) (4)
Info (4)	Info (LOG_INFO) (6)
Debug (5)	Debug (LOG_DEBUG) (7)

syslogd Configuration on the Switch

This procedure explains how to configure the switch to dispatch error log messages to a remote *syslogd* host.

To configure the switch to forward switch error log messages to a remote syslogd host:

1. Log in to the switch as admin user.
2. At the command line enter the `syslogdipadd` command using the following syntax:

   `switch:admin>syslogdipadd` "IP address of the remote syslogd host"
3. Verify the IP address was entered correctly using the `syslogdipshow` command.

Example The following example shows how to configure the switch to dispatch error log messages to a remote syslogd host whose IP address is 192.168.148.189

```
switch:admin> syslogdipadd 192.168.148.189
switch:admin> syslogdipshow
syslog.IP.address.1 192.168.148.189
```

To disable sending of error log messages to a previously enabled remote syslogd host:

1. Log in to the switch as Admin user.
2. At the command line enter the `syslogdipremove` command using the following syntax:

   `switch:admin>syslogdipremove "IP address of the remote syslogd host"`
3. Verify the IP address was deleted using the `syslogdipshow` command.

Example The following example shows how to disable sending of error log messages to a previously configured remote syslogd host whose IP address is 192.168.148.189:

```
switch:admin> syslogdipremove 192.168.148.189
```

syslogd Configuration on the Remote Host

The syslogd configuration on the UNIX host provides the syslogd daemon with instructions on how to process different messages it receives from the switch. The following are example entries in the syslog configuration file, /etc/syslog.conf, on how to store switch error log messages received from the switch. Please refer syslog related manual pages on your UNIX system for the full documentation of the syslog configuration file.

The following entry in /etc/syslog.conf causes all messages from the switch of UNIX priority warning or higher (that is, warning, error, critical and panic messages) to be stored in the file `/var/adm/emc`

Example

```
kern.warning /var/adm/emc
```

The following entry in /etc/syslog.conf causes all messages (Debug, Info, Warning, Error, Critical, and Panic) from the switch to be stored in the file `/var/adm/emc`

Example

```
kern.debug /var/adm/emc
```

The kern prefix identifies that the ED-12000B uses "kernel" syslogd facility to dispatch error log messages to the syslogd daemon.

syslogd CLI Commands

Below is a list of commands that are related to the syslogd configuration. Please refer to the help pages of these commands for more details.

Table 6-2 Commands Related to Syslogd Configuration

Command	Summary
syslogdipadd	Add the IP address of the remote syslogd host to the switch.
syslogdipremove	Remove the IP address of the remote syslogd deamon from the switch.
syslogdipshow	Show the list of configured syslogd IP addresses on the switch.
errshow	Display messages from the error log on the switch.

Solaris 8 Syslogd Functionality Changes

The Solaris syslogd functionality has changed between the Solaris 8 rev that ships on the installation CD and the latest patch. The change is that remotely generated *kernel* facility messages are sorted and logged as if they were *user* facility messages. This means that Solaris syslogd v1.84 and lower sort and log syslog messages from the switch properly with the following section in the /etc/syslog.conf file.

For switches running V4.x if the syslogd is v1.84 or lower:

```
kern.info/var/adm/core_info
kern.notice/var/adm/core_notice
kern.warning/var/adm/core_warning
kern.err/var/adm/core_err
kern.debug/var/adm/core_debug
kern.panic/var/adm/core_panic
kern.critical/var/adm/core_critical
```

For switches running V4.x if the syslogd is v1.87 or higher:

```
user.info/var/adm/core_info
user.notice/var/adm/core_notice
user.warning/var/adm/core_warning
user.err/var/adm/core_err
user.debug/var/adm/core_debug
user.panic/var/adm/core_panic
user.critical/var/adm/core_critical
```

Displaying the Switch Status

The switch status can be either Healthy/OK, Marginal/Warning, or Down. The overall status of a switch is determined by the status of several individual components within the switch. For more information about how the overall switch status is determined, refer to the `switchstatuspolicyset` command in the *Fabric OS Reference*.

To display the overall status of a switch:

1. Log in to the switch as the admin user.
2. Enter the `switchstatusshow` command. The status of the switch should be Healthy/OK. If the status is Marginal/Warning or Down, the components contributing to this status are displayed.

Example

```
switch:admin> switchstatusshow

The overall switch status is Marginal/Warning
Contributing factors:
* 1 bad power supply and 0 missing power supply triggered the Marginal/Warning
   status

switch:admin>
```

Displaying Information About a Switch

To display switch information:

1. Log in to the switch as the admin user.
2. Enter the `switchshow` command. This command displays the following information for a switch:
   - **switchName** - The switch's name
   - **switchType** - The switch's model and firmware version numbers.
   - **switchState** - The switch's state: Online, Offline, Testing, or Faulty.
   - **switchRole** - The switch's role: Principal, Subordinate, or Disabled.
   - **switchDomain** - The switch's Domain ID.
   - **switchId** - The switch's embedded port D_ID.
   - **switchWwn** - The switch's World Wide Name.
   - **switchBeacon** - The switch's beaconing state: either ON or OFF.

   This command also display the following information for ports on the specified switch:
   - **Module type** - The GBIC type if a GBIC is present.
   - **Port speed** - The speed of the Port (1G, 2G, N1, N2, or AN). The speed can be fixed, negotiated, or auto negotiated.
   - **Port state** - The port status.
   - **Comment** - Displays information about the port. This section may be blank or display WWN for F_port or E_port, Trunking state, upstream or downstream status.

Example The following example shows the output of the `switchshow` command on an DS-32B2.

```
switch:admin> switchshow
switchName: switch
switchType: 12.1
switchState: Online
switchRole: Principal
switchDomain: 2
switchId: fffc02
switchWwn: 10:00:00:60:69:90:02:84
switchBeacon:   OFF
```

```
Port Gbic Speed State
=========================
  0   id    N2   No_Light
  1   id    N1   Online    L-Port  2 public
  2   id    N2   No_Light
  3   --    N2   No_Module
  4   --    N2   No_Module
  5   id    N2   Online    L-Port  1 public
  6   --    N2   No_Module
  7   id    N2   No_Light
  8   id    N2   No_Light
  9   --    N2   No_Module
 10   --    N2   No_Module
 11   --    N2   No_Module
 12   id    N2   No_Light
 13   id    N2   No_Light
 14   id    N2   In_Sync
 15   id    N2   In_Sync
 16   --    N2   No_Module
 17   --    N2   No_Module
 18   --    N2   No_Module
 19   --    N2   No_Module
 20   --    N2   No_Module
 21   id    N2   No_Light
 22   id    N2   No_Light
 23   --    N2   No_Module
 24   id    N2   No_Light
 25   id    N2   No_Light
 26   id    N2   Online    F-Port  50:06:01:68:40:04:91:04
 27   --    N2   No_Module
 28   --    N2   No_Module
 29   --    N2   No_Module
 30   --    N2   No_Module
 31   --    N2   No_Module
```

Example The following example shows the output of the `switchshow` command on an ED-12000B.

```
switch12k:admin> switchshow
switchName:switch12k
switchType:10.1
switchState:Online
switchRole:Subordinate
switchDomain:2
switchId:fffc02
switchWwn:10:00:00:60:69:50:02:8f
switchBeacon:OFF
blade7: Beacon: OFF
Area Slot Port SFP Speed State
=====================================
 0    7    0   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94"
   (downstream)
```

```
  1    7    1   id    N2   Online     E-Port  10:00:00:60:69:00:54:e8 "san94"
  2    7    2   id    N2   Online     E-Port  10:00:00:60:69:00:54:e8 "san94"
  3    7    3   id    N2   Online     E-Port  10:00:00:60:69:00:54:e8 "san94"
  4    7    4   id    N1   Online     E-Port  10:00:00:60:69:12:34:e2 "san180"
  5    7    5   id    1G   No_Light
  6    7    6   --    1G   No_Module
  7    7    7   --    1G   No_Module
  8    7    8   --    1G   No_Module
  9    7    9   id    N2   Online     F-Port  21:00:00:e0:8b:04:1a:76
 10    7   10   id    N2   Online     E-Port  10:00:00:60:69:00:54:e8 "san94"
 11    7   11   id    N2   Online     E-Port  10:00:00:60:69:00:54:e8 "san94"
 12    7   12   --    1G   No_Module
 13    7   13   --    1G   No_Module
 14    7   14   id    N1   Online     E-Port  10:00:00:60:69:10:9b:06 "san176"
    (upstream)
 15    7   15   id    N2   Online     F-Port  10:00:00:00:c9:27:2e:69
switch12k:admin>
```

For more information refer to the `switchshow` command in the *Fabric OS Reference Manual*.

Displaying the Uptime of a Switch

To display the uptime for a switch:

1. Log in to the switch as the admin user.
2. Enter the `uptime` command. This command displays the current time, how long the system has been up, the number of users currently logged in, and the system load averages over the last 1, 5, and 15 minutes.

Example

```
switch:admin> uptime

 10:43am  up 19:42,  4 users,  load average: 0.01, 0.04,
   0.00

switch:admin>
```

Displaying the Status of a Port

There are two types of statistics you can view for a port:

- Software statistics
- Hardware statistics

Displaying Software Statistics for a Port

Software statistics for a port include information such as port state, number of interrupts, number of link failures, number of loss of synchronization warnings, and number of loss of signal warnings.

To display the software statistics for a port:

1. Log in to the switch as the admin user.
2. Enter the `portshow` command using the following syntax:

   `portshow [slotnumber/]portnumber`

   where *`slotnumber`* and *`portnumber`* indicates the port location you want to view.

   The slotnumber is for the ED-12000B only.

   A table of software statistics for the port is displayed.

Example The following example shows the software statistics displayed using the `portshow` command on a DS-32B2.

```
switch:admin> portshow 3
portCFlags: 0x1
portFlags: 0x20041       PRESENT U_PORT LED
portType:  4.1
portState: 2    Offline
portPhys:  4    No_Light
portScn:   0
portId:    010300
portWwn:   20:03:00:60:69:90:03:56
portWwn of device(s) connected:
        None
Distance:  normal
portSpeed: N2Gbps

Interrupts:        56          Link_failure: 6          Frjt:          0
Unknown:           0           Loss_of_sync: 0          Fbsy:          0
Lli:               16           Loss_of_sig:  1
Proc_rqrd:         40           Protocol_err: 0
```

```
Timed_out:          0          Invalid_word: 0
Rx_flushed:         0          Invalid_crc:  0
Tx_unavail:         0          Delim_err:    0
Free_buffer:        0          Address_err:  0
Overrun:            0          Lr_in:        3
Suspended:          0          Lr_out:       3
Parity_err:         0          Ols_in:       3
2_parity_err:       0          Ols_out:      3
CMI_bus_err:        0

switch:admin>
```

Example The following example shows the software statistics displayed using the `portshow` command on an ED-12000B.

```
switch:admin> portshow 7/3
portCFlags: 0x1
portFlags: 0x23801b      PRESENT ACTIVE F_PORT G_PORT LOGIN NOELP LED
   ACCEPT
portType:  4.1
portState: 1     Online
portPhys:  6     In_Sync
portScn:   6     F_Port
portId:    650300
portWwn:   20:03:00:60:69:00:54:e9
portWwn of device(s) connected:
        10:00:00:00:c9:24:0d:b3
Distance:  normal
portSpeed: N2Gbps

Interrupts:         36         Link_failure: 3          Frjt:         0
Unknown:            2          Loss_of_sync: 1          Fbsy:         0
Lli:                11         Loss_of_sig:  0
Proc_rqrd:          23         Protocol_err: 0
Timed_out:          0          Invalid_word: 0
Rx_flushed:         0          Invalid_crc:  0
Tx_unavail:         0          Delim_err:    0
Free_buffer:        0          Address_err:  0
Overrun:            0          Lr_in:        2
Suspended:          0          Lr_out:       2
Parity_err:         0          Ols_in:       2
2_parity_err:       0          Ols_out:      0
CMI_bus_err:        0

switch:admin>
```

For more information on the `portshow` command, refer to the *EMC Connectrix Departmental Switch DS-32B2B and Enterprise Director ED-12000B Fabric OS Reference Manual*.

Displaying Hardware Statistics for a Port

Hardware statistics for a port include information such as number of frames received, number of frames sent, number of encoding errors received, and number of class 2 and 3 frames received.

To display the hardware statistics for a port:

1. Log in to the switch as the admin user.
2. Enter the `portstatsshow` command using the following syntax:

   `portstatsshow slotnumber/portnumber`

   where `slotnumber` and `portnumber` is the port location you want to view.

   The slotnumber is for the ED-12000B only.

   A table of hardware statistics for the port is displayed.

Example The following example shows the hardware statistics displayed using the `portstatsshow` command on an ED-12000B.

```
switch:admin> portstatsshow 7/3
stat_wtx        353         4-byte words transmitted
stat_wrx        391         4-byte words received
stat_ftx        22          Frames transmitted
stat_frx        23          Frames received
stat_c2_frx     0           Class 2 frames received
stat_c3_frx     23          Class 3 frames received
stat_lc_rx      0           Link control frames received
stat_mc_rx      0           Multicast frames received
stat_mc_to      0           Multicast timeouts
stat_mc_tx      0           Multicast frames transmitted
tim_rdy_pri     0           Time R_RDY high priority
tim_txcrd_z     0           Time BB_credit zero
er_enc_in       0           Encoding errors inside of frames
er_crc          0           Frames with CRC errors
er_trunc        0           Frames shorter than minimum
er_toolong      0           Frames longer than maximum
er_bad_eof      0           Frames with bad end-of-frame
er_enc_out      2400        Encoding error outside of frames
er_disc_c3      0           Class 3 frames discarded
open            0           loop_open
transfer        0           loop_transfer
opened          0           FL_Port opened
```

```
starve_stop      0          tenancies stopped due to starvation
fl_tenancy       0          number of times FL has the tenancy
nl_tenancy       0          number of times NL has the tenancy
switch:admin>
```

For more information on the `portstatsshow` command, refer to the *EMC Connectrix Departmental Switch DS-32B2B and Enterprise Director ED-12000B Fabric OS Reference Manual.*

Displaying a Summary of Port Errors

The `porterrshow` command displays a summary of port errors for all the ports in a single switch.

To display a summary of port errors for a switch:

1. Log in to the switch as the admin user.
2. Enter the `porterrshow` command. The display contains one output line per port.

Example The following example displays the summary of port errors using the `porterrshow` command on an ED-12000B.

```
switch:admin> porterrshow
       frames    enc   crc  too   too  bad   enc  disc link loss loss frjt fbsy
      tx    rx    in   err  shrt  long eof   out   c3  fail sync  sig
    =====================================================================
 0:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
 1:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
 2:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
 3:   22    23     0     0    0     0    0  2.4k     0    3    1    0    0    0
 4: 144k   96k     0     0    0     0    0    19     0    1    0    0    0    0
 5: 142k   96k     0     0    0     0    0    19     0    1    0    0    0    0
 6: 141k   96k     0     0    0     0    0    19     0    1    0    0    0    0
 7: 145k   96k     0     0    0     0    0    18     0    1    0    0    0    0
 8:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
 9:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
10:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
11:    0     0     0     0    0     0    0     0     0    0    0    1    0    0
12:    0     0     0     0    0     0    0     0     0    0    0    1    0    0
13:    0     0     0     0    0     0    0     0     0    0    0    1    0    0
14:    0     0     0     0    0     0    0     0     0    0    0    1    0    0
15:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
32:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
33:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
34:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
35:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
36:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
37:    0     0     0     0    0     0    0     0     0    0    0    0    0    0
```

```
38:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
39:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
40:   95k  142k   0    0    0    0    0   55    0    1    0    0    0    0
41:   95k  141k   0    0    0    0    0   49    0    1    0    0    0    0
42:   95k  144k   0    0    0    0    0   40    0    1    0    0    0    0
43:   95k  140k   0    0    0    0    0   58    0    1    0    0    0    0
44:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
45:    0    0    0    0    0    0    0    0    0    0    0    0    0    0
46:    0    0    0    0    0    0    0    0    0    0    0    1    0    0
47:   31   39    0    0    0    0    0  6.9m   0    0   20    0    0    0
switch:admin>
```

The following table explains the types of errors counted:

Table 6-3 Error Summary Description

Error Type	Description
frames tx	Frames transmitted.
frames rx	Frames received.
enc in	Encoding errors inside frames.
crc err	Frames with CRC errors.
too shrt	Frames shorter than minimum.
too long	Frames longer than maximum.
bad eof	Frames with bad end-of-frame delimiters.
enc out	Encoding error outside of frames.
disc c3	Class 3 frames discarded.
link fail	Link failures (LF1 or LF2 states).
loss sync	Loss of synchronization.
loss sig	Loss of signal.
frjt	Frames rejected with F_RJT.
fbsy	Frames busied with F_BSY.

For more information on the `porterrshow` command, refer to the *EMC Connectrix Departmental Switch DS-32B2B and Enterprise Director ED-12000B Fabric OS Reference Manual*.

Displaying Fan Status

To display the fan status of a switch:

1. Log in to the switch as the admin user.
2. Enter the `fanshow` command. The possible values for fan status are:

   `OK` - Fan is functioning correctly.

   `Absent` - Fan is not present.

   `Below minimum` - Fan is present but rotating too slowly or stopped.

Example The following example displays the fan status using the `fanshow` command on a DS-32B2.

```
switch:admin> fanshow

Fan #1 is OK, speed is 3214 RPM
Fan #2 is OK, speed is 3245 RPM
Fan #3 is OK, speed is 3214 RPM
Fan #4 is OK, speed is 3308 RPM
Fan #5 is OK, speed is 3154 RPM
Fan #6 is OK, speed is 3341 RPM
switch:admin>
```

Example The following example displays the fan status using the `fanshow` command on an ED-12000B.

```
switch:admin> fanshow

Fan #1 is OK, speed is 2576 RPM
Fan #2 is OK, speed is 2500 RPM
Fan #3 is OK, speed is 2500 RPM
switch:admin>
```

The number of fans and valid range for RPMs varies depending on the type of switch. For more information, refer to the particular hardware reference manual for your switch.

Displaying Power Supply Status

To display the power supply status of a switch:

1. Log in to the switch as the admin user.
2. Enter the `psshow` command. The possible values for power supply status are:
   - **OK** - Power supply present and functioning correctly.
   - **Absent** - Power supply not present.
   - **Faulty** - Power supply present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

   After the status line, a power supply identification line may be shown. If present, this line contains manufacture date, part numbers, serial numbers, and other identification information.

Example The following example displays the power supply status using the `psshow` command on a DS-32B2.

```
switch:admin> psshow

Power Supply #1 is OK
0216,FF2H0000402,60-0000739-01, A,00011,SP467, F,FF2H0000402
Power Supply #2 is OK
0219,FF2Z0000258,60-0000739-01, A,,DCJ3002-01P,PP,FF2Z0000258
switch:admin>
```

Example The following example displays the power supply status using the `psshow` command on an ED-12000B.

```
switch:admin> psshow

Power Supply #1 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000931
Power Supply #2 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000925
Power Supply #3 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000941
Power Supply #4 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0130000942
switch:admin>
```

The number of Power Supply units varies depending on the type of switch. For more information, refer to the particular hardware reference manual for your switch.

Displaying Temperature Status

To display the temperature status of a switch:

1. Log in to the switch as the admin user.
2. Enter the `tempShow` command. This command displays current temperature readings from each of the five temperature sensors located on the main printed circuit board of the switch. The sensors are located, approximately, one in each corner and one at the center of the PCB.

Example The following example displays the temperature status using the `tempshow` command on a DS-32B2.

```
switch:admin> tempshow

Index   Slot    State           Centigrade      Fahrenheit
=========================================================
  1       0       Ok                43              109
  2       0       Ok                40              104
  3       0       Ok                22               71
  4       0       Ok                42              107
  5       0       Ok                39              102

switch:admin>
```

Example The following example displays the temperature status using the `tempshow` command on an ED-12000B.

```
   switch:admin> tempshow

Index   Slot    State           Centigrade      Fahrenheit
=========================================================
  1       1       Ok                46              114
  2       2       Absent
  3       3       Ok                42              107
  4       4       Absent
  5       5       Ok                23               73
  6       6       Ok                24               75

switch:admin>
```

The number of temperature sensors, the location of the sensors, and the range of temperatures for safe operation varies depending on the type of switch. For more information, refer to the particular hardware reference manual for your switch.

Running Diagnostic Tests on the Switch Hardware

There are several diagnostic tests you can run on a switch. The following tests are generally run during POST, which is performed each time a switch is booted up:

- camtest
- centralMemoryTest
- cmemRetentionTest
- cmiTest
- crossPortTest
- portLoopbackTest
- sramRetentionTest
- turboRamTest
- statsTest
- spinSilk

supportShow

Display status information of the switch and devices attached to the switch.

The output is very long. The supportShow command is used to gather switch information for debugging purposes. Your EMC Customer Support representative may ask you to run this command and capture the output. This information will aid Customer Service in diagnosing problems that could occur on the switch.

Syntax `supportShow [slot/Port1-Port2] [lines]`

The slotnumber is for the ED-12000B only.

Availability All users

Description Use this command to display multiple per selected Telnet user command results with a range of port specified in the user input

Operands This command has the following operands:

slot/port1-port2	Specify the range of ports within the blade specified by the slot to be displayed. Slot must be provided by ED-12000B only.
lines	Specify the number of lines for portlogdump output.

Example To display switch information for debugging:

```
switch:admin> supportShow 1/1-3
  version:
  Kernel:     2.4.2
  Fabric OS:  4.0.0t4Feb
  Made on:    Wed Feb 6 17:29:57 2002
  Flash:      Thu Jan 1 00:03:19 1970
  BootProm:   3.1.13b

  uptime:
   9:59pm  up  7 days, 4:25,  2 users,  load average: . . . .

  tempshow:

  Index   Slot     State          Centigrade     Fahrenheit
  ==========================================================
     1         1      Ok                  41         105
     2         2      Ok                  39         102
     3         3      Ok                  40         104

       ---< output truncated >---
```

7 Updating the Core PID Format

This chapter provides information about updating the Core Switch Port Identifier (PID) Format, including best practices for updating an existing production SAN to the new PID format.

In addition to the core PID format update process, there are a number of common scenarios in which a device may be assigned a new PID. Therefore the procedures included in this chapter are applicable to other areas of SAN administration, and should be generally useful to any SAN administrator. While this chapter is not comprehensive, it should provide a SAN administrator with the information required to plan and execute a successful core PID format update, and provide useful information for other SAN management tasks.

Overview

Updating the Core Switch PID Format is required when upgrading an existing SAN to support larger port-count switches. When a switch with more than 16 ports such as the DS-32B2 or the ED-12000B is introduced into an existing fabric, this parameter needs to be set on all switches in the fabric.

EMC recommends redundant fabrics and multi-pathing software for uptime-sensitive environments. If a redundant SAN architecture is in place, the Core PID update can take place without application downtime. To ensure maximum ease of administration, this parameter should be set on all switches in a fabric before the fabric enters production, regardless of whether an upgrade to larger switches is planned.

There are two addressing mechanisms used in Fibre Channel; Port Identifier (PID) and World Wide Name (WWN).

- A Port Identifier (PID) is analogous to specifying the physical switch and port to which a device is attached in a network; it is not analogous to an IP address. PIDs are assigned by a Fibre Channel switch when a device logs into the fabric, and a sample PID might look like the following: 011F00. There are numerous situations in which a device's PID may change.
- A WWN is analogous to an Ethernet MAC address. WWNs are assigned by the factory when a device is manufactured, and do not change. An sample WWN might look like the following: 10:00:00:60:69:51:0e:8b.

The method DS-8B, DS-16B, and DS-16B2 switches use to assign PIDs differs from the larger port count products.

The PID format is `XX1YZZ`:

- `XX` is the domain ID
- `1` is a constant (based on a conservative reading of the Fibre Channel standards)
- `Y` is a hexadecimal number which specifies a particular port on a switch
- `ZZ` is the AL_PA

The larger port count format is `XXYYZZ`:

- `XX` is the domain ID

- YY represents a port (using entire middle byte allows addressing up to 256 ports per switch)
- ZZ is the AL_PA

When a switch with the larger port count format is introduced into an existing fabric, the core PID format must be set on all switches in the fabric to prevent segmentation. This does not require application downtime, if redundant fabrics are used. If redundant fabrics are not in use, it is necessary to schedule an outage for the fabric.

EMC recommends redundant fabrics and multi-pathing software for uptime-sensitive environments. If redundant fabrics are *not* used, there are numerous possible failure cases and even routine maintenance scenarios that can result in application downtime.

Examples of scenarios protected by redundant fabrics include:

- Add / move / change operations for devices or switches
- Major upgrades / changes to fabric architecture
- Physical disasters
- Changing the core PID format
- Changing any other fabric-wide parameters, for example ED_TOV
- Erroneous zoning changes / user error

For new fabrics, the PID format should always be set to the larger port count addressing method before the fabric enters production. When updating an existing SAN, there are several scenarios which must be evaluated before changing the PID format.

Proactively setting the core PID format on new fabrics is strongly recommended to save potential administrative effort later on. There is no difference in the behavior of a fabric with either PID format.

Some device drivers map logical disk drives to physical Fibre Channel counterparts by PID. An example in a Windows HBA driver is Drive E: = PID 011F00. Most drivers can either dynamically change PID mappings or use the WWN of the Fibre Channel disk for mapping, not the PID. For example, Drive E: = WWN 10:00:00:60:69:51:0e:8b.

For those few drivers that use static PID binding, when the format is changed (PID à 010F00), the mapping breaks and must be manually fixed. (The driver still has Drive E: = PID 011F00 but the actual device address is now 010F00.) This can be done by rebooting the host, or using a manual update procedure on the host. This is discussed in more detail in the following sections.

- *Collecting Data* on page 7-5 of this chapter discusses in more detail the process of updating to the new PID format. This starts with evaluating a production SAN to see which if any devices bind by PID. Then either an online or offline update procedure is chosen to perform the actual update.
- *Detailed Procedures for HP/UX and AIX* on page 7-14 provides examples of step-by-step instructions for certain PID-bound devices. These procedures are applicable to any of a broad class of routine maintenance tasks; indeed, they would apply to these devices in many scenarios with any Fibre Channel switch in any addressing mode.
- *Frequently Asked Questions* on page 7-18 provides a Q&A format to discuss the issues surrounding a core PID format update.

In the more typical case where WWN or dynamic PID binding is used, changing the device's PID does not affect the mapping, but before updating the PID format, it is necessary to determine whether or not any devices in the SAN bind by PID.

Important EMC strongly recommends against using drivers that bind by PID. There are several routine maintenance procedures which may result in a device receiving a new PID; examples include but are not limited to:

- Changing **Compatibility Mode** settings
- Changing switch domain IDs
- Merging fabrics
- Merging fabrics
- Updating the core PID format
- Using hot spare switch ports to deal with failures

In every case where devices bind by PID, any such procedure becomes difficult or impossible to execute without downtime. In some cases, device drivers allow the user to manually specify persistent bindings by PID. In these cases, such devices must be identified and an appropriate update procedure created. If possible, the procedure should involve changing from PID binding to WWN binding.

Collecting Data

The fabric must be evaluated to find any devices which bind to PIDs, determine how each device driver will respond to the PID format change, and determine how any multi-pathing software will respond to a fabric service interruption. If current details about the SAN are already available, it may be possible to skip the Data Collection step. If not, it is necessary to collect information about each device in the SAN. Any kind of device may be able to bind by PID; each device should be evaluated prior to attempting an online update. This information has broad applicability, since PID-bound devices are not able to seamlessly perform in many routine maintenance or failure scenarios.

Following is a non-comprehensive list of information to collect:

- HBA driver versions
- Fabric OS versions
- RAID array microcode versions
- SCSI bridge code versions
- Multi-pathing software versions
- HBA time-out values
- Multi-pathing software time-out values
- Kernel time-out values
- Configuration

Some device drivers do not automatically bind by PID, but allow the operator to manually create a PID binding. For example, persistent binding of PIDs to logical drives may be done in many HBA drivers. Make a list of all devices that are configured this way. If manual PID binding is in use, consider changing to WWN binding.

Following are some of the device types that may be manually configured to bind by PID:

- HBA drivers (persistent binding)
- RAID arrays (LUN access control)
- SCSI bridges (LUN mapping)

Data Analysis

Once you have determined the code versions of each device on the fabric, they must be evaluated to find out if any automatically bind by PID. It may be easiest to work with the support providers to get this information. If this is not possible, you may need to perform empirical testing. Most devices that are running up-to-date drivers do not bind by PID.

Binding by PID can create management difficulties in a number of scenarios. EMC recommends using up-to-date drivers that do not bind by PID. If the current drivers do bind by PID, EMC recommends upgrading to WWN-binding drivers if possible.

The drivers shipping by default with HP/UX and AIX at the time of this writing still bind by PID, and so detailed procedures are provided for these operating systems on page 7-14. Similar procedures can be developed for other operating systems that run HBA drivers that bind by PID.

There is no inherent PID binding problem with either AIX or HP/UX. It is the HBA drivers shipping with these operating systems that bind by PID. Both operating systems are expected to release HBA drivers that bind by WWN, and these drivers may already be available through some support channels. Work with the appropriate support provider to find out about driver availability.

It is also important to understand how multi-pathing software reacts when one of the two fabrics is taken offline. If the time-outs are set correctly, the switchover between fabrics should be transparent to the users.

Empirical Testing

Empirical testing may be required for some devices, to determine whether they bind by PID. If you are not sure about a device, work with the support provider to create a test environment.

Create as close a match as practical between the test environment and the production environment, and perform an update using the Online Update procedure, provided above. Devices that bind by PID are unable to adapt to the new format, and one of three approaches must be taken with them:

- A plan can be created for working around the device driver's limitations in such a way as to allow an online update. See the detailed procedures section on page 7-14 for examples of how this could be done.
- The device can be upgraded to drivers that do not bind by PID.
- Downtime can be scheduled to reset the device during the core PID update process, which generally allows the mapping to be rebuilt.

If either of the first two options are used, the procedures should again be validated in the test environment.

Determine the behavior of multi-pathing software, including but not limited to:

- HBA time-out values
- Multi-Pathing software time-out values
- Kernel time-out values

Planning the Update Procedure

Whether it is best to perform an offline or online update depends on the uptime requirements of the site.

- An offline update requires less advance planning than an online update. However, it requires that all devices attached to the fabric be offline.
- With careful planning, testing, and general due-diligence, it should be safe to update the core PID format parameter in a live, production environment. This requires dual fabrics with multi-pathing software. Avoid running backups during the update process, as tape drives tend to be very sensitive to I/O interruption. The online update process is only intended for use in `uptime-critical dual-fabric environments, with multi-pathing software` (high-uptime environments should always use a redundant fabric SAN architecture). Schedule a time for the update when the least critical traffic is running.

All switches running any version of Fabric OS 4.x are shipped with the Core Switch PID Format enabled, so it is not necessary to perform the PID format change on these switches.

Migrating from manual PID binding (such as persistent binding on an HBA) to manual WWN binding and/or upgrading drivers to versions that do not bind by PID can often be done before setting the core PID format. This reduces the number of variables in the update process.

Outline for Online Update Procedure

The following steps are intended to provide SAN administrators a starting point for creating site-specific procedures.

1. Back up all data and verify backups.
2. If there is doubt as to whether the multi-pathing software can automatically switchover between fabrics seamlessly, use the software's administrative tools to manually disassociate or mark offline all storage devices on the first fabric to be updated.
3. Verify that I/O continues over the other fabric.
4. Disable all switches in the fabric to be updated, one switch at a time, and verify that I/O continues over the other fabric after each switch disable.
5. Change the PID format on each switch in the fabric (procedure provided below).
6. Re-enable the switches in the updated fabric, one switch at a time. In a core/edge network, enable the core switches first.
7. Once the fabric has re-converged, use the `cfgenable` command to update zoning (procedure provided below).
8. For any devices manually bound by PID, update their bindings. This may involve changing them to the new PIDs, or preferably changing to WWN binding.
9. For any devices automatically bound by PID, two options exist:
   a. Execute a custom procedure to rebuild its device tree online. Examples are provided in the Detailed Procedures section of this chapter.
   b. Reboot the device to rebuild the device tree. Some operating systems require a special command to do this, for example "boot –r" in Solaris.
10. For devices that do not bind by PID or have had their PID binding updated, mark online or re-associate the disk devices with the multi-pathing software and resume I/O over the updated fabric.
11. Repeat with the other fabric(s).

Outline for Offline Update Procedure

The following steps are intended to provide SAN administrators a starting point for creating site-specific procedures.

1. Schedule an outage for all devices attached to the fabric.
2. Back up all data and verify backups.
3. Shut down all hosts and storage devices attached to the fabric.
4. Disable all switches in the fabric.
5. Change the PID format on each switch in the fabric (procedure provided below).
6. One at a time, re-enable the switches in the updated fabric. In a core/edge network, enable the core switches first.
7. Once the fabric has re-converged, use the `cfgenable` command to update zoning (procedure provided below).
8. Bring the devices online in the order appropriate to the SAN. This usually involves starting up the storage arrays first, and the hosts last.
9. For any devices manually bound by PID, bring the device back online, but do not start applications. Update their bindings and reboot again if necessary. This may involve changing them to the new PIDs, or may (preferably) involve changing to WWN binding.
10. For any devices automatically bound by PID, reboot the device to rebuild the device tree (some operating systems require a special command to do this, such as "boot –r" in Solaris).
11. For devices that do not bind by PID or have had their PID binding updated, bring them back up and resume I/O.
12. Verify that all I/O has resumed correctly.

Hybrid Update

It is possible to combine the online and offline methods for fabrics where only a few devices bind by PID. Since any hybrid procedure is extremely customized, it is necessary to work closely with the SAN service provider in these cases.

Procedure for Updating the Core PID Format

This process should be executed as part of the overall online or offline update process. However, it may be implemented in a stand-alone manner on a non-production fabric, or a switch that has not yet joined a fabric.

1. Ensure that all switches in the fabric are running Fabric OS versions that support the new addressing mode. Check the EMC Support Matrix for the most current firmware revisions.

   All switches running any version of Fabric OS 4.x are shipped with the Core Switch PID Format enabled, so it is not necessary to perform the PID format change on these switches.

2. Telnet into one of the switches in the fabric.
3. Disable the switch by entering the `switchdisable` command.
4. Enter the `configure` command (the configure prompts display sequentially).
5. Enter **y** after the **Fabric parameters** prompt.
6. At the **Core Switch PID Format** prompt, enter **1**.
7. Complete the remaining prompts or press CTRL-D to accept the remaining settings without completing all the prompts.
8. Re-enable the switch by entering the `switchenable` command.
9. Repeat steps 2 through 8 for the remaining switches in the fabric.

Example

```
switch:admin> switchdisable
switch:admin> configure
Configure...
   Fabric parameters (yes, y, no, n): [no] yes

    Domain: (1..239) [1]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    SYNC IO mode: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0]
    Core Switch PID Format: (0..1) [0] 1
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..27) [16]
```

```
    Virtual Channel parameters (yes, y, no, n): [no]
    Switch Operating Mode (yes, y, no, n): [no]
    Zoning Operation parameters (yes, y, no, n): [no]
    RSCN Transmission Mode (yes, y, no, n): [no]
    Arbitrated Loop parameters (yes, y, no, n): [no]
    System services (yes, y, no, n): [no]
    Portlog events enable (yes, y, no, n): [no]
Committing configuration...done.
switch:admin> switchenable
```

10. Once all switches are updated to use the new PID format and re-enabled, verify that the fabric has fully re-converged (each switch sees the other switches).

Important

To prevent segmentation, it is critical that the fabric be completely re-converged before continuing with the next step.

11. Enter **cfgenable** [active_zoning_config] on one of the switches in the fabric to update zoning to use the new PID format. This does not change the definition of zones in the fabric, but merely causes the lowest level tables in the zoning database to be updated with the new PID format setting. It is only necessary to do this once per fabric; the zoning update automatically propagates to all switches.

    At this point, all switches in the fabric are operating in the new addressing mode.

Detailed Procedures for HP/UX and AIX

These procedures are not intended to be comprehensive. They provide a starting point from which a SAN administrator could develop a site-specific procedure for a device that binds automatically by PID, and cannot be rebooted due to uptime requirements.

HP/UX Procedure

1. Back up all data. Verify backups.
2. If you are not using multi-pathing software, stop all I/O going to all volumes connected through the switch/fabric to be updated.
3. If you are not using multi-pathing software, unmount the volumes from their mount points using umount. The proper usage would be `umount <mount_point>`. For example:

   ```
   umount /mnt/jbod
   ```

4. If you are using multi-pathing software, use that software to remove one fabric's devices from its configuration.
5. Deactivate the appropriate volume groups using `vgchange`. The proper usage would be `vgchange -a n <path_to_volume_group>`. For example:

   ```
   vgchange -a n /dev/jbod
   ```

6. Make a backup copy of the volume group directory using tar from within `/dev`. For example:

   ```
   tar -cf /tmp/jbod.tar jbod
   ```

7. Export the volume group using `vgexport`. The proper usage would be `vgexport -m <mapfile> <path_to_volume_group>`. For example:

   ```
   vgexport -m /tmp/jbod_map /dev/jbod
   ```

8. Log in to each switch in the fabric.
9. Issue the `switchDisable` command.
10. Issue the `configure` command and change the Core Switch PID Format to `1`.

11. Issue the command `cfgEnable [effective_zone_configuration]`. For example:

    ```
    cfgEnable my_zones
    ```

12. Issue the `switchEnable` command. Enable the core switches first, then the edges.
13. Clean the `lvmtab` file by using the `vgscan` command.
14. Change `to /dev` and untar the file that was tared in step 4. For example:

    ```
    tar -xf /tmp/jbod.tar
    ```

15. Import the volume groups using `vgimport`. The proper usage would be:
    `vgimport -m <mapfile> <path_to_volume_group> <physical_volume_path>`. For example:

    ```
    vgimport -m /tmp/jbod_map /dev/jbod /dev/dsk/c64t8d0
      /dev/dsk/c64t9d0
    ```

16. Activate the volume groups using `vgchange`. The proper usage would be `vgchange -a y <path_to_volume_group>`. For example:

    ```
    vgexport -a y /dev/jbod
    ```

17. If you are not using multi-pathing software, mount all devices again and restart I/O. For example:

    ```
    mount /mnt/jbod
    ```

18. If you are using multi-pathing software, re-enable the affected path. The preceding steps do not "clean up" the results from `ioscan`. When viewing the output of ioscan, notice the that the original entry is still there, but now has a status of NO_HW.

Example

```
# ioscan -funC disk
Class       I   H/W Path                    Driver S/W State      H/W Type          Description
-------------------------------------------------------------------------------------------------
disk        0   0/0/1/1.2.0                 adisk CLAIMED         DEVICE            SEAGATE ST39204LC
                                            /dev/dsk/c1t2d0 /dev/rdsk/c1t2d0
disk        1   0/0/2/1.2.0                 adisk CLAIMED         DEVICE            HP   DVD-ROM 304
                                            /dev/dsk/c3t2d0 /dev/rdsk/c3t2d0
disk        319 0/4/0/0.1.2.255.14.8.0      adisk CLAIMED         DEVICE            SEAGATE ST336605FC
                                            /dev/dsk/c64t8d0 /dev/rdsk/c64t8d0
disk        320 0/4/0/0.1.18.255.14.8.0     adisk NO_HW           DEVICE            SEAGATE ST336605FC
                                            /dev/dsk/c65t8d0 /dev/rdsk/c65t8d0
```

19. To remove the original (outdated) entry, the `rmsf` command (remove special file) will be needed. The proper usage for this command would be `rmsf -a -v <path_to_device>`. For example:

    ```
    rmsf -a -v /dev/dsk/c65t8d0
    ```

20. Validate that the entry has been removed by using the `ioscan -funC disk` command. Notice in the figure below that the NO_HW entry is no longer listed.

```
het46 (HP-50001)> ioscan -funC disk
Class       I   H/W Path                    Driver S/W State     H/W Type         Description
-------------------------------------------------------------------------------------------
disk        0   0/0/1/1.2.0                 adisk CLAIMED        DEVICE           SEAGATE ST39204LC
                                            /dev/dsk/c1t2d0 /dev/rdsk/c1t2d0
disk        1   0/0/2/1.2.0                 adisk CLAIMED        DEVICE           HP       DVD-ROM
    304
                                            /dev/dsk/c3t2d0 /dev/rdsk/c3t2d0
disk        319 0/4/0/0.1.2.255.14.8.0      adisk CLAIMED        DEVICE           SEAGATE ST336605FC
                                            /dev/dsk/c64t8d0 /dev/rdsk/c64t8d0
```

21. Repeat for all fabrics.

AIX Procedure

1. Back up all data. Verify backups.
2. If you are not using multi-pathing software, stop all I/O going to all volumes connected through the switch or fabric to be updated.
3. If you are not using multi-pathing software, varyoff the volume groups. The command usage is `varyoffvg <volume_group_name>`. For example:

    ```
    varyoffvg datavg
    ```

4. If you are not using multi-pathing software, unmount the volumes from their mount points using umount. The command usage is `umount <mount_point>`. For example:

    ```
    umount /mnt/jbod
    ```

5. If you are using multi-pathing software, use that software to remove one fabric's devices from its configuration.
6. Remove the device entries for the fabric you are migrating. For example, if the HBA for that fabric is fcs0, execute the command:

    ```
    rmdev -Rdl fcs0
    ```

7. Log in to each switch in the fabric.
8. Issue the `switchDisable` command.

9. Issue the `configure` command and change the Core Switch PID Format to `1`.
10. Issue the `configenable [effective_zone_configuration]` command. For example:

    ```
    configenable my_config
    ```

11. Issue the `switchEnable` command. Enable the core switches first, then the edges.
12. Rebuild the device entries for the affected fabric using the `cfgmgr` command. For example:

    ```
    cfgmgr -v
    ```

    This command may take several minutes to complete.

13. If you are not using multi-pathing software, vary on the disk volume groups. The proper usage would be `varyonvg <volume_group_name>`. For example:

    ```
    varyonvg datavg
    ```

14. If you are not using multi-pathing software, mount all devices again and restart I/O. For example:

    ```
    mount /mnt/jbod
    ```

15. If you are using multi-pathing software, re-enable the affected path.
16. Repeat for all fabrics.

Frequently Asked Questions

Q: What is a PID?
A: A PID is a Port Identifier. PIDs are used by the routing and zoning services in Fibre Channel fabrics to identify ports in the network. They are not used to uniquely identify a device; the World Wide Name (WWN) does that.

Q: What situations can cause a PID to change?
A: Many scenarios cause a device to receive a new PID. For example, unplugging the device from one port and plugging it into a different port (this might happen when cabling around a bad port, or when moving equipment around). Another example is changing the domain ID of a switch, which might be necessary when merging fabrics, or changing compatibility mode settings.

Q: Why do some devices handle a PID change well, and some poorly?
A: Some older device drivers behave as if a PID uniquely identifies a device. These device drivers should be updated if possible to use WWN binding instead. A device's WWN never changes, unlike its PID. PID binding creates problems in many routine maintenance scenarios, and should always be avoided. Fortunately, very few device drivers still behave this way, and these are expected to be updated as well.

Q: Must I schedule downtime for my SAN to perform the PID update?
A: Only if you do not have dual-fabrics or have devices that bind by PID.

Q: Must I stop all traffic on the SAN before performing the update?
A: If you are running dual-fabrics with multi-pathing software, you can update one fabric at a time. Move all traffic onto one fabric in the SAN, update the other fabric, move the traffic onto the updated fabric, and update the final fabric. Without dual-fabrics, stopping traffic is highly recommended. This is the case for many routine maintenance situations, so dual-fabrics are always recommended for uptime-sensitive environments.

Q: How can I avoid having to change PID formats on fabrics in the future?

A: The core PID format can be proactively set on a fabric at initial installation. The update could also be opportunistically combined with any scheduled outage. Setting the format proactively far in advance of adoption of higher port count switches is the best way to ensure administrative ease.

8 Troubleshooting

This chapter provides information on troubleshooting and the most common procedures used to diagnose and repair issues. In this chapter:

The following specific scenarios are described to provide examples of Troubleshooting techniques:

About Troubleshooting

Troubleshooting should begin at the center of the SAN — the fabric. Because switches are located between the hosts and storage devices, and have visibility into both sides of the storage network, starting with them can help narrow the search path. After eliminating the possibility of a fault within the fabric, see if the problem is on the storage side or the host side, and continue a more detailed diagnosis from there. Using this approach can quickly pinpoint and isolate problems.

For example, if a host cannot see a storage device, run a switch command to see if the storage device is logically connected to the switch. If not, focus first on the storage side. Use storage diagnostic tools to better understand why it is not visible to the switch. Once the storage can be seen from the switch, if the host still cannot see the storage device, then there is still a problem between the host and switch.

Fibre Channel Process

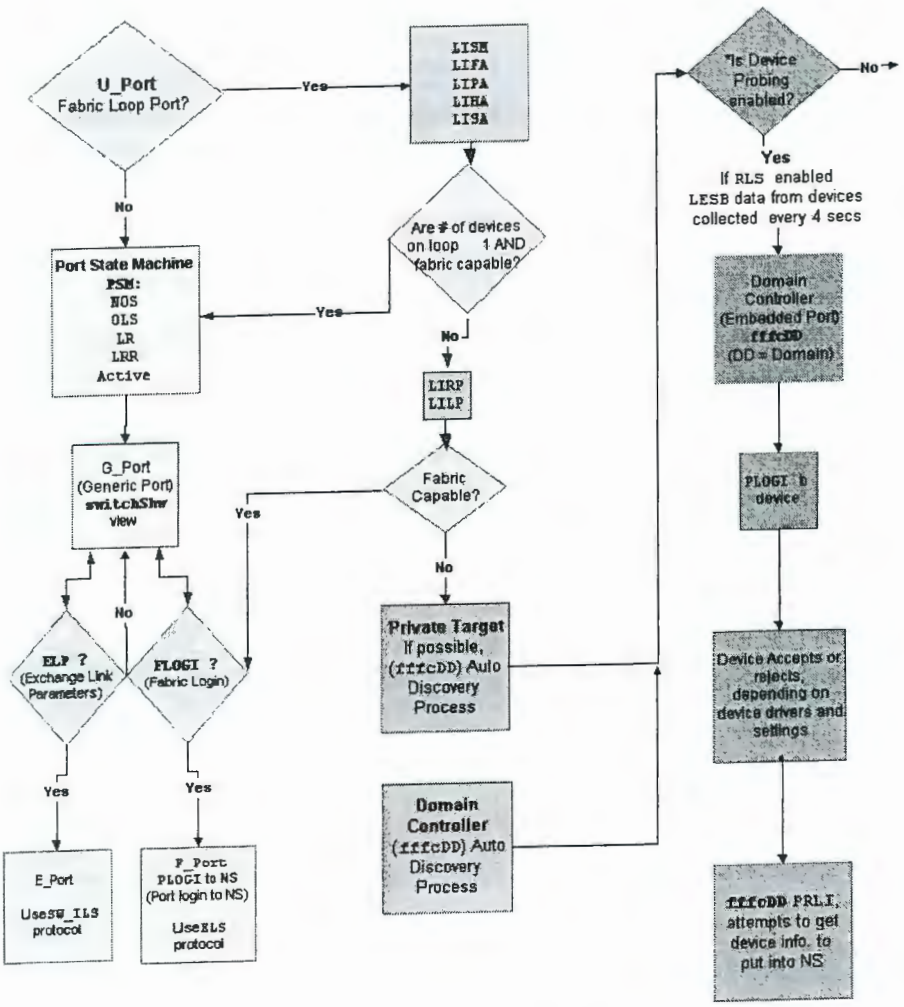


Figure 8-1 Fibre Channel Process Flow Chart

Most Common

Table 8-1 Most Common Problem Areas

Area	Investigate
Fabric	Missing devices
	Marginal links (unstable connections)
	Incorrect zoning configurations
	Incorrect switch configurations
Storage Devices	Physical issues between switch and devices
	Incorrect storage software configurations
Hosts	Incorrect host bus adapter installation
	Incorrect device driver installation
	Incorrect device driver configuration
Storage Management Applications	Incorrect installation and configuration of the storage devices that the software references. For example, if using a volume-management application, check for: ◆ Incorrect volume installation ◆ Incorrect volume configuration

Problem Areas

There are many tools available to help troubleshoot the SAN. The following table describes tools that can be used to troubleshoot specific areas.

Table 8-2 Troubleshooting Tools

Problem Area	Troubleshooting Tool
Fabric	Switch LEDs.
	Switch commands for diagnostics (command line).
	Web or GUI-based monitoring and management software tools.
	Real-time distributed fabric operating system with advanced diagnostics.
Storage Devices	Device LEDs
	Storage diagnostic tools
Hosts	Host adaptor LEDs
	Host operating system diagnostic tools
	Device driver diagnostic tools
Storage Management Applications	Application-specific tools and resources

Gathering Information for EMC Technical Support

To aid in troubleshooting, gather as much of this information as possible prior to contacting EMC Technical Support.

1. Gather Switch Information:
   a. Serial number (located on the chassis).
   b. Worldwide name (obtain using **licenseidshow** or **wwn** commands)
   c. Fabric OS version (obtain using **version** command)
   d. Switch Configuration settings
2. Gather Host Information:
   a. OS version and patch level
   b. HBA type
   c. HBA firmware version
   d. HBA driver version
   e. Configuration settings
3. Gather Storage Information:
   a. Disk/tape type
   b. Disk/tape firmware level
   c. Controller type
   d. Controller firmware level
   e. Configuration settings
4. Storage Software (i.e., EMC ControlCenter, Veritas SPC, etc.)
5. SNMP management being used

Specific Scenarios

The following sections provides specific help with some of the most common SAN problems.

Host Can't See Target (Storage or Tape Devices)

When a host cannot "see" its disks, the best way to troubleshoot the problem is to start in the middle half of the data path, figure out if the problem is "above" or "below" the data path, and keep dividing the suspect path in half until the problem is identified.

There are a few areas to check in the process of elimination:

- *Check the Logical Connection*
- *Check the Simple Name Server (SNS)*
- *Check for Zoning Discrepancies*
- Check Device Communication.

Check the Logical Connection

Check Whether the Device is Logically Connected to the Switch

1. Enter the **switchShow** command.
2. Review the output and determine if the device is logically connected to the switch:
   - A device that *is* logically connected to the switch will be registered as an NX_Port.
   - A device that is *not* logically connected to the switch will be registered as something *besides* an NX_Port.
     a. If the missing device *is* logically connected, move on to *Check for the Device in the SNS*.
     b. If the missing device is *not* logically connected, eliminate the host and everything on that side of the data path from the suspect list.
     This includes all aspects of the host's OS, the HBA driver settings and binaries, the HBA Basic Input Output System (BIOS) settings, the HBA SFP, the cable going from the switch to the host, the SFP on the switch side of that cable, and all switch settings related to the host. Move on to *Link Initialization Failure (Loop)*.

Check the Simple Name Server (SNS)

Check for the Device in the SNS

1. Enter the **nsShow** command on the switch to which the device is attached.

```
The Local Name Server has 9 entries {
 Type Pid    COS     PortName                NodeName                TTL(sec)
*N    021a00;    2,3;20:00:00:e0:69:f0:07:c6;10:00:00:e0:69:f0:07:c6; 895
     Fabric Port Name: 20:0a:00:60:69:10:8d:fd
NL    051edc;     3;21:00:00:20:37:d9:77:96;20:00:00:20:37:d9:77:96; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL    051ee0;     3;21:00:00:20:37:d9:73:0f;20:00:00:20:37:d9:73:0f; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL    051ee1;     3;21:00:00:20:37:d9:76:b3;20:00:00:20:37:d9:76:b3; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL    051ee2;     3;21:00:00:20:37:d9:77:5a;20:00:00:20:37:d9:77:5a; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL    051ee4;     3;21:00:00:20:37:d9:74:d7;20:00:00:20:37:d9:74:d7; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL    051ee8;     3;21:00:00:20:37:d9:6f:eb;20:00:00:20:37:d9:6f:eb; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 NL    051eef;     3;21:00:00:20:37:d9:77:45;20:00:00:20:37:d9:77:45; na
     FC4s: FCP [SEAGATE ST318304FC       0005]

     Fabric Port Name: 20:0e:00:60:69:10:9b:5b
 N     051f00;    2,3;50:06:04:82:bc:01:9a:0c;50:06:04:82:bc:01:9a:0c; na
     FC4s: FCP [EMC      SYMMETRIX       5267]

     Fabric Port Name: 20:0f:00:60:69:10:9b:5b
```

2. Look for the device in the list of the Simple Name Server. The SNS lists all of the nodes connected to that switch, which allows a user to determine if a particular node is accessible on the network.

If the device is *not* present in the SNS, the search is narrowed to the virtual SAN cable; the problem is between the storage device and the switch. This is not a host problem, and may indicate a timeout or communication problem between the edge device(s) and the Name Server. Move on to step 3.

If the device *is* listed in the SNS, the search is narrowed; the problem is between the storage device and the host. There may be a zoning mismatch or a host/storage issue. Refer to *Check for Zoning Discrepancies*.

3. Check the edge device documentation to determine if there is a timeout setting or parameter that may be re-configured. If this does not solve the communication problem, contact the support organization for the product that appears to be timing out.

Check for Zoning Discrepancies

To determine if zoning might be causing a communication problem between devices:

1. Enter the **cfgShow** command to determine if zoning is enabled.

   If zoning is enabled, it is possible that the problem is being caused by a zoning conflict. (i.e. two devices in different zones cannot see each other).

Example

```
switch:admin> cfgshow
Defined configuration:
  cfg:    USA1     Blue_zone
  cfg:    USA_cfg Red_zone; Blue_zone
  zone:   Blue_zone
     1,1; array1; 1,2; array2
  zone:   Red_zone
     1,0; loop1
  alias: array1   21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
  alias: array2   21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
  alias: loop1    21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
  cfg:    USA_cfg
  zone:   Blue_zone
      1,1
      21:00:00:20:37:0c:76:8c
      21:00:00:20:37:0c:71:02
      1,2
      21:00:00:20:37:0c:76:22
      21:00:00:20:37:0c:76:28
   zone:   Red_zone
      1,0
      21:00:00:20:37:0c:76:85
      21:00:00:20:37:0c:71:df
```

2. Confirm that the specific edge devices that need to communicate with each other are in the same zone.
   - If they are, zoning is not causing the communication problem.
   - If they are not, and zoning is enabled, continue to step 3
3. Resolve zoning conflicts by putting the devices into the same zoning configuration.

   Refer to *Basic Zone Merge Correction Procedure*.

Fabric Segmentation

Possible Causes

Fabric Segmentation is generally caused by:

- Incompatible fabric parameters. Refer to *Restore a Segmented Fabric*
- The Core PID is not set. The Core PID is part of fabric parameters. Refer to Chapter 7, *Updating the Core PID Format*.
- Incompatible zoning configuration. Refer to *Fabric Merge Conflicts Related to Zoning*.
- Domain ID conflict. Refer to *Reconcile a Domain ID Conflict*.
- A switch in a secure fabric is not running Secure Fabric OS. Refer the *Secure Fabric OS User's Guide*.

About Fabric Parameters

There are a number of settings that control the overall behavior and operation of the fabric. Some of these values, such as the domain ID, are assigned automatically by the fabric and may differ from one switch to another in the fabric. Other parameters, such as the BB credit, can be changed for specific applications or operating environments, but must be the same among all switches to allow the formation of a fabric.

Mandatory Identical Settings

The following fabric parameters must be identical for a fabric to merge:

- R_A_TOV
- E_D_TOV
- Data Field Size
- Sequence Level Switching
- Disable Device Probing
- Suppress Class F Traffic
- VC Encoded Address Mode
- Per-frame Route Priority
- Long Distance Fabric
- BB Credit
- Core PID

Domain ID Conflicts

A domain ID conflict can occur if a switch that is in the online state is added to a fabric, and the joining switch domain ID conflicts with the domain ID of a switch in the fabric. Normally, domain IDs are automatically assigned; however, once a switch is online, the domain ID cannot change, as it would change the port addressing and potentially disrupt critical I/O.

Restore a Segmented Fabric

The following procedure describes how to check for inconsistent fabric parameters that cause segmentation. For information on zoning configuration incompatibility, refer to *Fabric Merge Conflicts Related to Zoning*.

Reconcile Fabric Parameters Individually

The following procedure describes how to edit incompatible fabric parameters between fabrics by hand. To reconcile an entire configuration at once, refer to *Restore Fabric Parameters Through ConfigUpload*.

1. Log in to one of the segmented fabrics as admin.
2. Enter the **configshow** command.
3. Open another telnet session and log in to the next fabric as admin.
4. Enter the **configshow** command.
5. Compare the two fabric configurations line by line and look for differences. Do this by comparing the two telnet windows, or by printing the **configshow** output.
6. Log in to the segmented switch once the discrepancy is identified.
7. Disable the switch by entering **switchdisable**.
8. Enter the **configure** command to edit the fabric parameters for the segmented switch.

   Refer to the *Fabric OS Reference Guide* for more detailed information.
9. Enable the switch by entering the **switchenable** command.

Restore Fabric Parameters Through ConfigUpload

The following procedure describes how to restore a segmented fabric by uploading the entire "correct" configuration, then downloading that configuration to the segmented switch. This reconciles any discrepancy in the fabric parameters and allows the segmented switch to rejoin the main fabric. To edit and correct a configuration by hand, refer to *Reconcile Fabric Parameters Individually*.

1. Verify that the FTP service is running on the host workstation.
2. Log in to a switch in the known working fabric as admin.
3. Run the **configupload** command.
4. Name the text file something relevant and save it to a host.
5. Open a new telnet session and log in to the segmented switch as admin.
6. Shut down the switch by entering the **switchdisable** command.
7. Enter **configdownload** at the command line. The command becomes interactive and prompts appear for the required information.
8. Select "y" at the *Do you want to continue* [y/n] prompt.

   A *download complete* message displays.
9. (Optional) Use the **configure** command to preset the domain ID (as opposed to letting it be chosen at random).
10. Reboot the switch by entering the **reboot** command.
11. Repeat this procedure on all switches that have incorrect fabric parameters.

Reconcile a Domain ID Conflict

When a domain ID conflict appears, the conflict is only reported at the point where the two fabrics are physically connected. However, there may be several conflicting domain IDs, which will appear as soon as the initial conflict is resolved. Repeat the process described below until all domain ID conflicts are resolved.

1. Enter the **switchshow** command on a switch from one of the fabrics.
2. Open a separate telnet window.
3. Enter the **switchshow** command on a switch from the second fabric.
4. Compare the **switchshow** output from the two fabrics. Note the number of domain ID conflicts; there may be several duplicate domain IDs that will need to be changed.
5. Chose the fabric on which to change the duplicate domain ID; log in to the conflicting switch in that fabric.
6. Enter the **switchdisable** command.

7. Enter the **switchenable** command.

   This will enable the joining switch to obtain a new domain ID as part of the process of coming online. The fabric principal switch will allocate the next available domain ID to the new switch during this process.

8. Repeat steps 5 - 7 if additional switches have conflicting domain IDs.

Zoning Setup Issues

Zoning Related Commands

Table 8-3 Zoning Related Commands

Command	Function
switchshow	Displays currently enabled configuration and any E_port segmentations due to zone conflicts.
licenseshow	Displays current license keys and associated (licensed) products.

Table 8-4 Zone Specific Commands

Command	Function
cfgcreate	Use to create a zone configuration.
cfgshow	Displays zoning configuration.
zoneadd	Use to add a member to an existing zone.
zoneshow	Displays zone information.
zonecreate	Use to create a zone. Before a zone becomes active, the **zonesave** and **cfgenable** commands must be used.
alicreate	Use to create a zone alias.
alidelete	Use to delete a zone alias.
zonehelp	Displays help information for zone commands.

Refer to the *Zoning User's Guide* for information about setting up zoning and preventing segmentation due to zoning.

Fabric Merge Conflicts Related to Zoning

Prevention

To prevent fabric segmentations, refer to the *Zoning User's Guide* for setup information. In addition, fabric merges can be tested prior to merging using Fabric Manager. Refer to the *Fabric Manager User's Guide*.

There are three types of zone configuration discrepancies that can cause segmentation, described in Table 8-5.

Table 8-5 Types of Zone Discrepancies

Conflict Cause	Description
Configuration mismatch	Occurs when Zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.
Type mismatch	Occurs when the name of a zone object in one fabric is also used for a different type of zone object in the other fabric.
Content mismatch	Occurs when the definition of a zone object in one fabric is different from the definition of a zone object with the same name in the other fabric.

Basic Zone Merge Correction Procedure

CAUTION

This is a disruptive procedure. To correct a merge conflict without disrupting the fabric, refer to *Detailed Zone Merge Correction Procedure* or the *Zoning User's Guide*.

To quickly correct a fabric merge problem due to incompatible zones, perform the following steps:

1. Determine which switch(es) have the incorrect configuration; log in to that switch as admin.

2. Enter the **cfgDisable** command.
3. Enter the **cfgClear** command.

CAUTION

Be careful in using the cfgclear command because you can inadvertently delete the Zone configuration in the fabric. Make sure you are deleting the "incorrect" configuration.

4. Enter the **switchdisable** command.
5. Enter the **switchenable** command. This automatically evokes the **cfgSave** command.

   The two fabrics will be remerged.
6. Refer to *Detailed Zone Merge Correction Procedure* for more detailed troubleshooting instructions.

Detailed Zone Merge Correction Procedure

For more information regarding Zoning, refer to the *Zoning User's Guide*.

For detailed troubleshooting of zone merge issues, follow the steps below:

1. Verify Fabric Merge Problem

1. Enter the **swithshow** command at the command line to validate that the segmentation is due to a zone issue.
2. Refer to *Zoning Setup Issues* to view the different types of zone discrepancies.

2. Edit Zone Config Members

1. Log in to one of the segmented Fabrics as admin.
2. Enter the **cfgshow** command.

   Typing the "*" symbol after the command displays list of all config names.
3. Print the output from the **cfgShow** command.
4. Start another Telnet session and log in to the next fabric as admin.
5. Run the **cfgShow** command.
6. Print the output from the **cfgShow** command.
7. Compare the two fabric zone configurations line by line and look for incompatible configuration. Refer to *Fabric Merge Conflicts Related to Zoning* for definitions.

8. Log in to one of the Fabrics.
9. Run zone configure edit commands to edit the fabric zone configuration for the segmented switch. Refer to the *Zoning User's Guide* for specific commands.

3. Reorder the Zone Member List

If the zoneset members between two switches are not listed in the same order in both configurations, the configurations are considered a mismatch; this results in the switches being segmented in the fabric. For example:

`[cfg1 = z1; z2]` is different from `[cfg1 = z2; z1]`, even though the members of the configuration are the same.

One simple approach to making sure that the zoneset members are in the same order is to keep the members in alphabetical order.

1. Use the output from the **cfgshow** for both switches.
2. Compare the order that the zone members are listed. Members must be listed in the same order.
3. Rearrange zone members so that the configuration for both switches is the same. Arrange zone members in alphabetical order, if possible.
4. Continue to the next step if all zone members appear to be the same, and are displayed in the same order.

MQ-WRITE Error

An MQ error is a message queue error. Identify an MQ error message by looking for the two letters M and Q in the error message.

```
<switch number> Critical MQ-QREAD, 1, mqRead, queue = <?>, queue ID = <queue ID#>,
tmsg = ?>, errno = <error number>
```

MQ errors can result in devices dropping from the Simple Name Server or can prevent a switch from joining the fabric. MQ errors are rare and difficult to troubleshoot, and it is suggested that they be resolved by working with the switch supplier. When MQ errors are encountered, execute the **supportShow** command to capture debug information about the switch. Then forward the **supportShow** data to the switch supplier for further investigation.

I2C bus Errors

Possible Causes

i2C bus errors indicate defective hardware, and the specific item is listed in the error message. Refer to the *Diagnostics and Error Messages Guide* for information specific to the error that was received. Specifically, some CPT and Environmental Monitor (EM) messages contain i2C-related information.

Troubleshooting the Hardware

If the i2C message does not indicate the specific hardware that may be failing, begin debugging the hardware, as this is the most likely cause.

Check Fan Components

1. Log in to the switch as User.
2. Enter **fanshow** at the command line.
3. Check the Fan status and speed output.

   If any of the fan speeds display abnormal RPMs, replace the fan FRU.

Check the Switch Temperature

1. Log in to the switch as User.
2. Enter **tempshow** at the command line.
3. Check the temperature output.

   Look for indications of high or low temperatures.

Check the Power Supply

1. Log in to the switch as User.
2. Enter the **psshow** command at the command line.
3. Check the power supply status. Refer to the *Fabric OS Reference Guide* or the appropriate *Hardware Reference* for details regarding the power supply status.

   If any of the power supplies show a status other than OK, consider replacing the power supply as soon as possible.

Check the Temperature, Fan, and Power Supply

1. Log in to the switch as User.
2. Enter **sensorshow** at the command line. Refer to the *Fabric OS Reference Guide* for details regarding the sensor numbers.
3. Check the temperature output.

   Look for indications of high or low temperatures.

4. Check the Fan speed output.

   If any of the fan speeds display abnormal RPMs, replace the fan FRU.

5. Check the Power Supply status.

   If any of the power supplies show a status other than OK, consider replacing the power supply as soon as possible.

Device Login Issues

In narrowing down problems with device logins, use the following commands:

1. Log in to the switch.
2. Enter the **switchShow** command. Check for correct logins.

Example

```
switch:admin> switchshow
switchName:     switch
switchType:     16.2
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   7
switchId:       fffc07
switchWwn:      10:00:00:60:69:c0:0e:88
switchBeacon:   OFF
Zoning:         ON (cfg1)
port  0: id N2 Online         E-Port 10:00:00:60:69:c0:0f:04 "web189" (upstream)

port  1: id N2 No_Light
port  2: id N2 No_Light
port  3: id N2 No_Light
port  4: id N2 No_Light
port  5: id N2 No_Light
port  6: id N2 No_Light
port  7: id N2 No_Light
switch:admin>
```

3. Enter the **portconfigShow** command to see how the port is configured.

Example

```
switch:admin> portcfgshow
Ports                0  1  2  3    4  5  6  7
-------------------+--+--+--+--+----+--+--+--
Speed               2G 2G 2G 2G   2G 2G 2G 2G
Trunk Port          .. .. ON ON   ON ON ON ON
Long Distance       .. .. .. ..   .. .. .. ..
VC link init        .. .. .. ..   .. .. .. ..
Locked L_Port       .. .. .. ..   .. .. .. ..
Locked G_Port       .. .. .. ..   .. .. .. ..
Disabled E_Port     .. .. .. ..   .. .. .. ..
Persistent Disable  .. .. .. ..   .. .. .. ..
ISL R_RDY Mode      .. .. .. ..   ON .. ON ..
                   where AN:AutoNegotiate, ..:OFF, ??:INVALID.
                         LM:L0.5
switch:admin>
```

4. Enter the **portErrShow** command. Check for errors that may cause login problems.
   - A high number of errors relative to the frames transmitted and frame received may indicate a marginal link. Refer to *Marginal Links*.
   - A steadily increasing number of errors may indicate a problem. Track errors by sampling the port errors every five or ten seconds.

Example

```
switch:admin> portflagsshow
Port SNMP       Physical    Flags
--------------------------------
  0: Offline    No_Module   PRESENT U_PORT LED
  1: Offline    No_Module   PRESENT U_PORT LED
  2: Offline    No_Light    PRESENT U_PORT LED
  3: Offline    No_Light    PRESENT U_PORT LED
  4: Offline    No_Light    PRESENT U_PORT LED
  5: Offline    No_Module   PRESENT U_PORT LED
  6: Offline    No_Module   PRESENT U_PORT LED
  7: Offline    No_Module   PRESENT U_PORT LED
  8: Offline    No_Module   PRESENT U_PORT LED
  9: Offline    No_Module   PRESENT U_PORT LED
 10: Offline    No_Module   PRESENT U_PORT LED
 11: Offline    No_Module   PRESENT U_PORT LED
 12: Offline    No_Module   PRESENT U_PORT LED
 13: Offline    No_Module   PRESENT U_PORT LED
 14: Offline    No_Module   PRESENT U_PORT LED
 15: Offline    No_Module   PRESENT U_PORT LED
 16: Online     UNKNOWN     PRESENT ACTIVE G_PORT U_PORT
switch:admin>
```

5. Enter the **portFlagsShow** command to see how a port has logged in and where a login failed, if a failure occurred.

Example

```
 13: Online     In_Sync     PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB L
OGIN LED
 14: Online     In_Sync     PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB L
OGIN LED
 15: Online     In_Sync     PRESENT ACTIVE F_PORT L_PORT U_PORT LOGIN NOELP LED AC
CEPT
 16: Online     In_Sync     PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB L
OGIN LED
```

6. Enter the **portlogdumpport** [, *saved*[, *portid*]]

   View the device to switch communication.

Example

```
switch:admin> portlogdump 41
time          task       event   port cmd  args
-----------------------------------------------
16:44:21.490  PORT       Rx        41   40  02ffffd,00ffffd,0005ffff,14000000
16:44:21.490  PORT       Tx        41    0  c0ffffd,00ffffd,00050541
16:44:32.503  PORT       Tx        41   40  02ffffd,00ffffd,0542ffff,14000000
16:44:32.506  PORT       Rx        41    0  c0ffffd,00ffffd,05420006
16:44:35.993  PORT       Rx         5   40  02ffffd,00ffffd,0a49ffff,14000000
16:44:35.993  PORT       Tx         5    0  c0ffffd,00ffffd,0a490543
16:44:35.997  PORT       Tx         5   40  02ffffd,00ffffd,0544ffff,14000000
16:44:36.000  PORT       Rx         5    0  c0ffffd,00ffffd,05440a4a
16:44:42.340  PORT       Rx        41   40  02ffffd,00ffffd,0009ffff,14000000
16:44:42.340  PORT       Tx        41    0  c0ffffd,00ffffd,00090545
switch:admin>
```

Watchdog (Best Practices)

Watchdog is a subset of the Kernel Error Reporting Software; it is a feature that reports unexpected and fatal errors when a switch dies. The Watchdog feature ensures that the switch will not send corrupted data when the software is not properly performing its function.

The ASIC has a Watchdog register that needs to be probed by the Fabric OS once every two seconds. If the ASIC detects that the Fabric OS is hung, the ASIC will wait for an additional two seconds before resetting the CPU. The switch will always reboot or fail over when a Watchdog error occurs.

Actions

In the event of a Watchdog error, perform the following steps:

- Collect the output of the **supportshow** command and contact EMC Technical Support.
- (Optional) Turn on **settasklogmode** in the event of a Watchdog error; this will allow more information to be collected. Do not enable this mode by default as it will slow traffic.
- See specific error message for additional actions. Refer to *Kernel Software Watchdog Related Errors*.

Kernel Software Watchdog Related Errors

kSWD-APP_NOT_REFRESH_ERR

Message

```
Critical kSWD-APP_NOT_REFRESH_ERR, 1, (kSWD)Application with pid <PID number> not
refreshing watchdog.
```

Explanation A critical kernel software error occurred in the Watch Dog subsystem. An kernel application is not able to refresh. Refer to the specified PID number to find out which application is failing. The switch will reboot (on single-CP switches) or fail-over (on dual-CP switches).

Action Run the **savecore** command to find if a Core File was created. If a Core File is found, select the *FTP the file* option.

Copy the error message and contact customer support.

Severity Critical

kSWD-kSWD_GENERIC_ERR_CRITICAL

Message

```
Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: <error string>
```

Explanation A critical application error was reported in the Watch Dog subsystem. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or fail-over (on dual-CP switches).

Action Run the **savecore** command to find out whether a Core File was created. If a Core File is found, select the *FTP the file* option.

Copy the error message and contact customer support.

Severity Critical

Identifying Media-Related Issues

Use the following section to narrow down media-related issues in the fabric.

Component Tests Overview

Hardware diagnostics available on switches can be classified into two different types of tests:

- Structural tests - do basic tests of the switch circuit. When structural tests fail, replace the mainboard.
- Functional tests - verify the intended operational behavior of the switch by running frames through ports or bypass circuitry.

Table 8-6 Component Test Descriptions

Test Name	Operands	Checks
crossporttest	[**-nframes** *count*] [**-lb_mode** *mode*][**-spd_mode** *mode*] [**-gbic_mode** *mode*] [**-norestore** *mode*] [**-ports** *itemlist*]	Functional test of port external transmit and receive path. The **crossport** is set to loopback using an external cable by default. However, this command can be used to check internal components by setting the *lb* operand to 5.
fporttest	[**-nframes** *count*] [**-ports** *itemlist*] [**-seed** *payload_pattern*] [**-width** *pattern_width*] [**-size** *pattern_size*]	Tests component to / from HBA. Used to test online F_Port devices, N_Port devices and SFPs/GBICs.
loopporttest	[**-nframes** *count*] [**-ports** *itemlist*][**-seed** *payload_pattern*] [**-width** *pattern_width*]	Only tests components attached to switch that are on a FC arbitrated loop.
spinfab	[*nMillionFrames* [, *ePortBeg* [, *ePortEnd* [, *setFail*]]]]	Tests components to/from a neighbor switch, such as ISLs and SFPs/GBICs between switches.

Check Switch Components

Cursory Debugging of Media Components

The following procedure describes basic steps that can help to narrow down faulty media.

1. Log in to the switch as admin.
2. Enter **switchshow** at the command line.

   Look for a known good portstate online or insync.
3. (Optional) Enter **version** at the command line.

   The version can be used to check the known buglist in the appropriate Release Notes.
4. Enter **portErrShow** at the command line.

   A error summary of all ports is displayed.
5. Glance over the port statistics.
   - Most numbers should be small. An excessively large number (such as one over 100,000) could indicate a bad transceiver.
   - Also check for rapidly rising error counts.

   Tip: The LLI_errs (Low Level Interrupt_errors) are the sum of the port's 8 statistical error counters: ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3. Check **portErrShow** output to determine what generated LLI_errs.
6. (Optional) Run tests if you still suspect a media problem.
   - To test components to and from a neighbor switch, refer to *Test Cascaded Switch ISL Links.*
   - To test a ports external transmit and receive path, refer to *Check Port's External Transmit and Receive Path.*
   - To test the internal components of a suspect switch, refer to *Test a Switches Internal Components.*
   - To test the components between a switch and a hub (and back), refer to *Test Components To and From the HBA.*
   - To check all switches attached components (on an FC loop), refer to *Check All Switch Components Between Main Board, SFP, and Fibre Cable.*
   - To check all of a port's attached components (on an FC loop), refer to *Check Port's External Transmit and Receive Path.*

- To view a list of additional component tests, refer to *Additional Component Tests*.

Test Cascaded Switch ISL Links

To tests components to/from a neighbor switch:

7. Log in to the switch as admin.
8. Enter the **spinfab** command with the following operands (refer to the *Fabric OS Reference Guide* for more details):

[**-nmegs** *count*]	Specify the number of frames to send in millions.
[**-ports** *list*]	(Optional) Specify a list of user ports to test.
[**-setfail** *mode*]	Specify a value 1 to mark failing ports as BAD, specify a value of 0 to *not* mark failed ports as bad.
[**-domain** *value*]	(Optional) Specify a specific remote domain to which the switch is connected.

```
switch:admin> setdbg "DIAG", 0
switch:admin> spinfab 3,0,4

spinFab running...

spinFab: Completed 3 megs, status:  passed.
        port 0 test status: 0x00000000 --  passed.
        port 1 test status: 0x00000000 --  passed.
        port 2 test status: 0x00000000 --  passed.
        port 3 test status: 0x00000000 --  passed.
        port 4 test status: 0x02000000 --  SKIPPED!

switch:admin> setdbg "DIAG", 2
switch:admin> spinfab 3,0,3

spinFab running...
port  1 Rx  1 million frames.
port  0 Rx  1 million frames.
port  2 Rx  1 million frames.
port  3 Rx  1 million frames.
port  1 Rx  2 million frames.
port  0 Rx  2 million frames.
port  2 Rx  2 million frames.
port  3 Rx  2 million frames.
port  1 Rx  3 million frames.
port  0 Rx  3 million frames.
port  2 Rx  3 million frames.
port  3 Rx  3 million frames.

spinFab: Completed 3 megs, status:  passed.
        port 0 test status: 0x00000000 --  passed.
        port 1 test status: 0x00000000 --  passed.
        port 2 test status: 0x00000000 --  passed.
        port 3 test status: 0x00000000 --  passed.

switch:admin>
```

Test a Ports External Transmit and Receive Path

9. Log in to the switch as admin.
10. Enter the **crossporttest** command with the following operand

    (This is a partial list. Refer to the *Fabric OS Reference Guide* for more information):

[**-nframes** *count*]	Specify the number of frames to send.
[**-lb_mode** *mode*]	Select the loopback point for the test.
[**-spd_mode** *mode*]	Select the speed mode for the test.
[**-ports** *itemlist*]	Specify a list of user ports to test.

```
switch:admin> crossporttest
Running Cross Port Test .... passed.
```

Test a Switches Internal Components

To use the **crossporttest** to test a switches internal components:

1. Log in to the switch as admin.
2. Enter the **crossporttest -lb_mode 5** command.

   Where *5* is the operand that causes the test to be run on the internal switch components.

   (This is a partial list. Refer to the *Fabric OS Reference Guide* for more information):

   [-nframes *count*] Specify the number of frames to send.

   [-lb_mode *mode*] Select the loopback point for the test.

   [-spd_mode *mode*] Select the speed mode for the test.

   [-ports *itemlist*] Specify a list of user ports to test.

Test Components To and From the HBA

1. Log in to the switch as admin.
2. Enter the **fPortTest** command with the following operands (refer to the *Fabric OS Reference Guide* for details):

   [*passCount*] Specify the number of times (or number of frames per port) to execute this test (default is infinite or until enter key is hit)

   [*port_number*] Specify the port on which to run to test (F_Port by default).

   [*payload_pattern*] Specify the pattern of the test packets payload.

   [pattern_width] Specify the width of the pattern which user specified - it could be 1, 2, or 4 (which are byte, word, or quad)

   [*pattern_size*] Specify the number of words in test packet payload (default is 512)

```
switchname:admin> fPortTest 100,8,0xaa55,2, 512
 Will use pattern: aa55  aa55  aa55 aa55  aa55  aa55 ...
 Running fPortTest ........
 port 8 test passed.
 value = 0
```

The example above executed **fPortTest** 100 times on port 8 with payload pattern 0xaa55, pattern width 2 (meaning word width) and default payload size 512 bytes.

Check All Switch Components Between Main Board, SFP, and Fibre Cable

The following procedure exercises all the switch components from the main board --> SFP --> fibre cable --> SFP on the device --> back to main board.

1. Make sure all connected cables and SFPs are of the same technology (i.e. a short wavelength SFP switch port should be connected to another short wavelength device SFP through a short wavelength cable).
2. Log in to the switch as admin.
3. Determine which ports are L-Ports by entering the **switchshow** command.
4. Enable ports for loopback mode by entering **loopporttest** [**--slot** *number*] [**-nframes** *count*][**-ports** *itemlist*][**-seed** *payload_pattern*][**-width** *pattern_width*].

   Refer to the *FOS Command Reference* for more information about the operands.
5. Create a frame F of data size (1024) bytes.
6. Transmit frame F via port M, with D_ID to the FL port (AL_PA = 0).
7. Pick up the frame from port M, the FL port.
8. Determine if any of the following statistic error counters are non-zero:

   `ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.`
9. Determine if the transmit, receive, or class 3 receiver counters are stuck at a value.

10. Determine if the number of frames transmitted is not equal to the number of frames received.
11. Repeat steps 3 through 11 for all L-ports present until:
    a. the number of frames requested is reached
    b. all ports are marked bad
12. Look for errors. See the list below for possible errors.

Possible Errors

One or more of the following errors may appear if failures are detected. Refer to the *Diagnostics and Error Messages Guide* to find details and actions for any errors that appear.

```
DATA
INIT
PORT_DIED
EPI1_STATUS_ERR
ERR_STAT
ERR_STATS_2Long
ERR_STATS_BADEOF
ERR_STATS_BADOF
ERR_STATS_C3DISC
ERR_STATS_CRC
ERR_STATS_ENCIN
ERR_STATS_ENCOUT
ERR_STATS_TRUNC
ERR_STAT_2LONG
ERR_STAT_BADEOF
ERR_STAT_BADOS
ERR_STAT_C3DISC
ERR_STAT_CRC
ERR_STAT_ENCIN
ERR_STAT_ENCOUT
ERR_STAT_TRUNC
FDET_PERR
FINISH_MSG_ERR
FTPRT_STATUS_ERR
MBUF_STATE_ERR
MBUF_STATUS_ERR
NO_SEGMENT
PORT_ABSENT
PORT_ENABLE
PORT_M2M
PORT_STOPPED
PORT_WRONG
RXQ_FAM_PERR
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FTX
```

```
TIMEOUT
XMIT
```

Check Port's External Transmit and Receive Path

The following procedure exercises the path of a loop from the port N transmitter, along the parallel loopback path, and back to the same N port transmitter. Loopback adapters are optional for this test.

This test does *not* exercise the SFP or the fibre cable. This test only checks components that are attached to the switch and that are on a FC arbitrated loop.

1. Log in as admin.
2. Disable the switch by entering **switchdisable** at the command line.
3. Enter **portloopbacktest** [*passcount*] to set all ports for parallel loopback.

   Refer to the *Fabric OS Reference Guide* for detailed information about the optional operand.
4. Transmit frame F through port N.
5. Pick up the frame from the same port N.
6. Check the following statistic error counters for non-zero values:

   ```
   ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_Out,
   BadOrdSet, DiscC3
   ```
7. Check if the transmit, receive, or class 3 receiver counter are stuck at a value.
8. Check if the number of frames transmitted is not equal to the number of frames received.
9. Repeat steps 3 - 7 for all ports present until:
   - The number of frames (or passCount) requested is reached.
   - All ports are marked as bad.

Possible Errors

One or more of the following errors may appear if failures are detected. Refer to the *Diagnostics and Error Messages Guide* to find details and actions for any errors that appear.

```
DIAG-INIT
DIAG-PORTDIED
DIAG_XMIT
DIAG-TIMEOUT
DIAG_ERRSTAT
DIAG-STATS
DIAG-DATA
```

Check all Switch Components of the Port Transmit and Receive Path

The following procedure exercises all the switch components from the main board --> SFP --> fibre cable --> back to SFP --> back to main board.

1. Make sure all cables used for connected port and SFPs are of the same technology (i.e. a short wavelength SFP switch port should be connected to another short wavelength device SPF through a short wavelength cable).
2. Connect ports from different ASICs, if possible (for example, connect port 1 - port 7).
3. Log in to the switch as admin.
4. Enter **switchdisable** *if* the switch should assume all ports are cable loopbacked (and test accordingly).

   or

   Leave the switch enabled if only cable loopbacked ports should be tested (and the rest ignored).
5. (Optional) Enter **setsfpmode** to limit the test to ports with that contain SFPs.

   This mode must be disabled when test is complete.
6. Enable the ports for cabled loopback mode by entering **crossporttest** with the selected operands.

   Refer to the *Fabric OS Reference Guide* for details regarding the operands.
7. Create a frame F of maximum data size (2112 bytes).
8. Transmit frame F through port M.
9. Pick up the frame from its cross connected port N. An error is reported if any port other than N actually receives the frame.
10. Determine if any of the following statistic error counters are non-zero:

    `ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.`
11. Determine if the transmit, receive, or class 3 receiver counters are stuck at a value.
12. Determine if the number of frames transmitted is not equal to the number of frames received.

13. Determine if the number of frames transmitted is not equal to the number of frames received.
14. Repeat steps 6 - 12 for all ports until:
    - the number of frames requested is reached.
    - all ports are marked bad.
15. (Optional) Disable SFP mode. If **setsfpmode** was entered, the mode remains it volatile memory until it is disabled. Enter **setsfpmode** 0.

Additional Component Tests

The following list displays additional tests that can be used to determine those switch components that are not functioning properly. Refer to the *Fabric OS Reference Guide* for details on these tests.

Table 8-7 Switch Component Tests

Test	Function
portloopbacktest	Functional test of port N->N path. Refer to *Check Port's External Transmit and Receive Path.*
portregtest	A read and write test of the ASIC SRAMs and registers.
spinsilk	Functional test of internal and external transmit and receive paths at full speed.
sramretentiontest	Verifies that data written into the miscellaneous SRAMs in the ASIC are retained after a 10 second wait.
crossporttest	Verifies the functional components of the switch.
turboramtest	Verifies the on chip SRAM located in the 2 Gbit/sec ASIC using the Turbo-Ram BIST circuitry. These same SRAMS are tested by **portregtest** and **sramretentiontest** using PCI operations, but for this test the BIST controller is able to perform the SRAM write and read operations at a much faster rate.

Table 8-7 Switch Component Tests

Test	Function
statstest	Verifies the 2 Gbit/sec ASIC statistics counter logic.
Related Switch Test Command:	
itemlist	List parameter syntax and grammar information; restricts the items to be tested to a smaller set the parameter values.

Link Failure

A link failure occurs when a server or storage is connected to a switch, but the link between the server/storage and the switch does not come up. This prevents the server/storage from communicating through the switch.

Possible Causes for Link Failure

If the **switchshow** command and/or the LED lights indicate that the link has not come up properly, follow the steps for one or more of the areas indicated below.

A link failure can be caused by one of the following reasons:

- *Switch State*
- *Port's Physical State*
- *Speed Negotiation Failure*
- *Link Initialization Failure (Loop)*
- *Port Has Come Up in a Wrong Mode*

Switch State

1. Enter the **switchshow** command.
2. Check the switchState entry in the **switchshow** command output.
3. Use the following list of switch states to determine the next step:

Table 8-8 SwitchState and Actions to Take

SwitchState	Action
Online	The state of the switch is ok. Move on to check the *Port's Physical State*.
Offline	Enable the switch by entering the **switchenable** command.
Testing	Wait for the switch to complete its test.
Faulty	Check the condition of the switch. Enter the **switchStatusShow** and **errShow** or **errDump** commands and identify the malfunctioning parts. Refer to the *Fabric OS Reference Guide* for more information.

Port's Physical State

4. Enter the **switchshow** command.

5. Check the port and state columns in the **switchshow** output.
6. Use the following list to determine the next step:

Table 8-9 Port States and Suggested Actions

Port State	
Online	The port physical state is OK. If the link has not come up, go to *Port Has Come Up in a Wrong Mode.*
No_Card	Check the SFP/GBIC.
No_Module	Check the SFP/GBIC.
No_Light	Check the physical contact and the cabling.
No_Sync	The port is receiving light but out of sync. Move on to *Speed Negotiation Failure.*
In_Sync	The port is in sync, but is not online. Move on to *Link Initialization Failure (Loop).*
Laser_Flt	Check the physical contact and the cabling.
Port_Flt	Check the physical condition of the port. Refer to *Identifying Media-Related Issues.*
Diag_Flt	Check the physical condition of the port. Enter the **diagShow** and **errShow** or **errDump** commands and identify the cause.
Testing	Wait for the completion of the test.

Speed Negotiation Failure

Skip this section if the port speed is set to a static speed through the **portCfgSpeed** command.

The port negotiates the link speed with the opposite side. The negotiant usually completes in 1-2 seconds; however, sometimes the speed negotiation fails.

Determine if the negotiation was successfully completed:

1. Enter the **portLogShow** or **portLogDump** command.
2. Check the events area of the output for the following information:

1 Gig example:

```
14:38:51.976  SPEE       sn       <Port#>   NC  00000001,00000000,00000001
```

2 Gig example:

```
14:39:39.227  SPEE       sn       <Port#>   NC  00000002,00000000,00000001
```

- The sn field indicates a speed negotiation.
- The NC field indicates Negotiation Complete.
- The 01 or 02 fields indicate the speed that has been negotiated.

If these fields do not appear, move on to the step 3.

3. Correct the negotiation by entering the **portCfgSpeed** [*slotnumber/*]*portnumber, speed_level* command if the fields above do not appear.

Link Initialization Failure (Loop)

1. Verify the port is an L_Port.
   a. Enter the **switchShow** command.
   b. Check the comment field of the output to verify that the switch port indicates an L_Port. If a loop device is connected to the switch, the switch port must be initialized as an L_Port.
2. Verify the loop initialization *if* the port is not an L_port.
   a. Enter the **portLogShow** or **portLogDump** command.
   b. Check the event area for a loopscn entry with command code BMP.

   Example:

```
14:35:12.866  tReceive   loopscn  <Port#>  BMP  10f5cbc0
```

   The loopscn entry display indicates that the loop initialization is complete.
3. Skip point-to-point initialization.

   SilkWorm switches the point-to-point initialization after the Loop Initialization Soft Assigned (LISA) phase of the loop initialization. This behavior sometimes causes trouble with old HBAs. If this is the case:

a. Skip point-to-point initialization by using the **portCfgLport** Command.

Point-to-Point Initialization Failure

1. Confirm that the port is active

   If a Fabric device or another switch is connected to the switch, the switch port must be active.

   a. Enter the **portLogShow** or **portLogDump** commands.

   b. Verify that the State Change Notification (SCN) code is 1. An SCN of 1 indicates that the port is active.

   Example:

```
13:25:12.506  PORT      scn      <Port#>    1
```

2. Skip over the loop initialization phase

   After becoming an active port, the port becomes an F_Port or an E_Port depending on the device on the opposite side. If the opposite device is a Fabric device, the port becomes an F_Port. If the opposite device is another switch, the port becomes an E_Port.

   Some Fabric devices have problem with loop initialization. If this is the case, perform the following step:

   a. Enter the **portCfgGport** command.

Port Has Come Up in a Wrong Mode

1. Enter the **switchShow** command.
2. Check the comment fields for the following output and follow the suggested actions.

Table 8-10 SwitchShow Output and Suggested Action

Output	Suggested Action
Disabled	Enter the **portEnable** command.
Bypassed	Check the output from **portLogShow** or **portLogDump** commands and identify the link initialization stage where the initialization procedure went wrong.
Loopback	Check the output from portLogShow/PortLogDump commands and identify the link initialization stage where the initialization procedure went wrong.

Table 8-10 SwitchShow Output and Suggested Action

Output	Suggested Action
E_port	If the opposite side is not another switch, the link has come up in a wrong mode. Check the output from portLogShow/PortLogDump commands and identify the link initialization stage where the initialization procedure went wrong.
F_port	If the opposite side of the link is a fabric device, the link has come up in a wrong mode. Check the output from **portLogShow** or **PortLogDump** commands.
G_port	The port has not come up as an E_port or F_port. Check the output from **portLogShow** or **PortLogDump** commands and identify the link initialization stage where the initialization procedure went wrong.
L_port	If the opposite side is *not* a loop device, the link has come up in a wrong mode. Check the output from **portLogShow** or **PortLogDump** commands and identify the link initialization stage where the initialization procedure went wrong.

Marginal Links

A marginal link involves the connection between the switch and the edge device. Isolating the exact cause of a marginal link involves analyzing and testing many of the components that make up the link: switch port, switch SFP, cable, the edge device, and the edge device SFP.

Confirming the Problem

The following steps provide a brief overview of possible steps to troubleshoot a marginal link.

1. Enter the **portErrShow** command.

Example

```
switch:admin> porterrshow
       frames    enc   crc  too  too  bad  enc disc link loss loss frjt fbsy
     tx     rx    in   err shrt long  eof  out   c3 fail sync  sig
=============================================================================
 0:    22     24     0    0    0    0    0  1.5m    0    7    3    0    0    0
 1:    22     24     0    0    0    0    0  1.2m    0    7    3    0    0    0
 2:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
 3:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
 4:  149m    99m     0    0    0    0    0   448    0    7    6    0    0    0
 5:  149m    99m     0    0    0    0    0   395    0    7    6    0    0    0
 6:  147m    99m     0    0    0    0    0   706    0    7    6    0    0    0
 7:  150m    99m     0    0    0    0    0   160    0    7    5    0    0    0
 8:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
 9:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
10:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
11:     0      0     0    0    0    0    0     0    0    0    0    2    0    0
12:     0      0     0    0    0    0    0     0    0    0    0    2    0    0
13:     0      0     0    0    0    0    0     0    0    0    0    2    0    0
14:     0      0     0    0    0    0    0     0    0    0    0    2    0    0
15:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
32:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
33:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
34:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
35:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
36:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
37:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
38:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
39:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
40:   99m   146m     0    0    0    0    0   666    0    6  796    7    0    0
41:   99m   149m     0    0    0    0    0   15k    0    2  303    4    0    0
42:   99m   152m     0    0    0    0    0   665    0    2  221    5    0    0
43:   99m   147m     0    0    0    0    0   16k    0    2  144    4    0    0
44:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
45:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
46:     0      0     0    0    0    0    0     0    0    0    0    2    0    0
47:     0      0     0    0    0    0    0     0    0    0    0    0    0    0
switch:admin>
```

2. Establish if there are a relatively high number of errors (such as CRC errors or ENC_OUT errors), or if there are a steadily increasing number of errors to confirm a marginal link.

   If high errors exist, refer to step 1.

Isolating the Areas

1. Move the suspected marginal port cable to a different port on the switch.

- If the problem stops or goes away, the switch port or the SFP is marginal. Continue to step 2
- If the problem does *not* stop or go away, refer to *Ruling Out Cabling Issues* or *Nx_Port (Host or Storage) Issues*.

2. Replace the SFP on the marginal port.
3. Run the **portLoopBack** test on the marginal port. Refer to the *FOS Reference Guide* or *Troubleshooting the Hardware* for more information.
4. Check the results of the loopback test, and proceed as follows:
   - If the loopback test failed, the port is bad. Replace the port card.
   - If the loopback test did not fail, the SFP was bad.

Ruling Out Cabling Issues

1. Begin by performing the steps in *Isolating the Areas*.

   By now an SFP problem is ruled out.
2. Insert a new cable in to the suspected marginal port.
3. Enter the **portErrShow** command to determine if a problem still exists.
   - If the **portErrShow** output displays a normal number of generated errors, the issue is solved.
   - If the **portErrShow** output still displays a high number of generated errors, move on to *Nx_Port (Host or Storage) Issues*.

Nx_Port (Host or Storage) Issues

1. Begin performing the steps in *Isolating the Areas* and *Ruling Out Cabling Issues*.

   By now an SFP problem and a cable problem have been ruled out.
2. Follow the troubleshooting procedures for the Host or Storage device.

Switch Appears to "Hang"

If a switch appears to be "hung-up", or passing no data (including error messages to the serial portLog), it may indicate that the switch is being Flow Controlled by a terminal server. By default, Flow Control is disabled on v3.1 and v4.1 switches; however, if Flow Control has been enabled, it could cause a switch to hang.

Determining if a Switch is Being Flow Controlled

Flow Control is most likely causing a switch to "hang" if the following is true:

- A terminal server is connected to the serial port.
- The switch is *not* sending messages to the serial portLog.
- Flow Control has been enabled on the terminal server.

If the statements above are true, Flow Control from the terminal server is most likely preventing the switch from passing traffic. Refer to *Correcting a "Hung" Switch* to correct the problem.

Correcting a "Hung" Switch

If Flow Control has been enabled, and a switch is being flow-controlled by a terminal server (refer to Page 8-48), perform the following procedure:

1. Access the console.
2. Press Ctrl-Q to cause the terminal to re-enable flow.
3. Determine if flow control is enabled, using the appropriate commands for the terminal server or terminal emulator.
4. Disable Flow Control if it is enabled.

Using Flow Control can cause a switch to "hang" if it fails to manage the flow control properly, or manages it out of the expected sequence.

CAUTION

Though Flow Control may need to be disabled on the client device, disabling Flow Control *can* create a separate undesirable situation: unexpected or missing information in the serial portLog. Refer to *Correcting Serial PortLog Output*.

Unexpected Output in the Serial PortLog

Console serial port logs can sometimes appear to have incorrect, corrupt, or missing information due to potential overruns when connected to:

- terminal emulation programs
- terminal emulation devices
- concentrators

Correcting Serial PortLog Output

If your serial port is connected to terminal emulation programs or terminal emulation devices, perform the following steps:

1. Determine if your serial port is connected to terminal emulation/terminal servers/concentrators.
2. Access the console.
3. Determine if flow control is disabled, using the appropriate commands for the terminal server or terminal emulator. Flow Control is disabled by default for v3.1 and v4.1.

   If Flow Control is disabled, this is most likely causing the incorrect data in the serial portLog.
4. Enable Flow Control on the terminal server.

CAUTION

Though Flow Control may need to be enabled on the client device, use of flow control *can* create a separate, undesirable situation. Flow Control may cause the switch to appear to "hang" if the client device fails to manage the flow control properly, or manages it out of the expected sequence. Refer to *Switch Appears to "Hang"*.

Refer to *Switch Appears to "Hang"* for more Flow Control-related information.

Inaccurate Information in the Error Log

In rare instances, events gathered by the Track Change feature can report inaccurate information to the error log.

For information regarding enabling and disabling Track Changes (TC), refer to *Tracking Switch Changes*.

Inaccurate Login Reported by Track Changes

Scenario:

A user entered a correct user name and password, but the login was rejected because the maximum number of users had been reached. However, when looking at the error log, the login was reported as successful.

Explanation:

If the maximum number of switch users has been reached, the switch will still perform correctly in that it will reject the login of additional users (even if they enter correct user name and password information).

However, in this limited scenario, the Track Change feature will report this event inaccurately to the error log; it will appear that the login was successful. This scenario only occurs when the maximum number of users has been reached; otherwise, the login information displayed in the error log should reflect reality.

A

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure A-1).

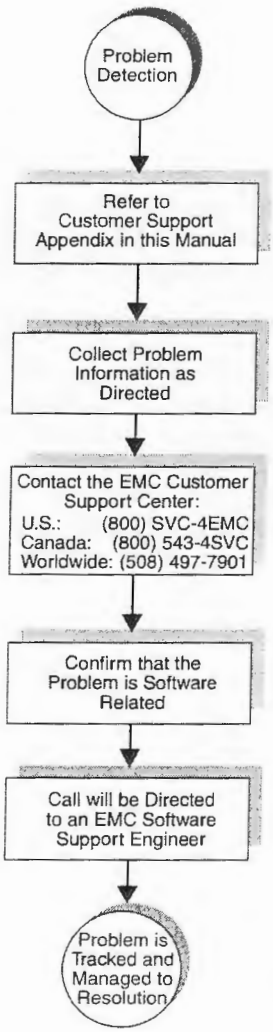


Figure A-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.emc.com`

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word — Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector — A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW — Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port — A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration — The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device — A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 — Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID — As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode.*

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit*.

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL*.

M

Media See *Transceiver*.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port*.

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

ANEXO SWITCH TIPO 03
PARTE 7

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

EMC²

RELEASE NOTES

EMC Connectrix ED-12000B and DS-32B2

Version 4.1.1

Release Notes

P/N 300-000-551
Rev A05

6/23/03

These release notes contain supplemental information about EMC Connectrix Enterprise Director ED-12000B and DS-32B2, version 4.1.1. Topics include:

General Information

The information in this document is a supplement to the documentation CD that was provided with the switch. However, information in these release notes supersedes any information found in earlier documentation.

Fabric OS 4.1 represents the second major feature release of firmware for the ED-12000B and DS-32B2 switches. This release adds a large number of significant new features to an already robust and comprehensive firmware platform.

Fabric OS 4.1 represents the first major feature revision to the Fabric OS v4.0 firmware. It should be considered an upgrade and replacement for Fabric OS 4.0.

Obtaining Software Updates

Contact EMC Global Services for software updates and maintenance releases. New switch firmware can be installed from the following host operating systems:

- UNIX
- Linux
- Windows NT
- Windows 2000
- Windows 98
- Windows 95

The ED-12000B supports the following optional software products:

- Zoning
- Web Tools
- ISL Trunking
- Fabric Watch
- Performance Monitoring

The above products can be activated with the purchase of the applicable license key.

MIB Files and Fabric Watch Profiles

To access sample MIB files and Fabric Watch configurations for switch management by SNMP on the EMC website:

1. Go to the Powerlink website:

   `http://www.powerlink.emc.com`

2. Select **Services**, **Document Library**, **Connectrix**.

3. Scroll down to the desired files.

MIB Files

The following MIB files are supported:

- `v4_0FA.mib` Supports Fibre Alliance MIB v3.0
- `v4_0FA.mib` `v4_0FE.mib` is the same as `festd.smiv2` in v3.0 and refers to RFC 2837
- `v4_0SW.mib` Connectrix Fibre Channel Switch MIB v4.0
- `v4_0TRP.mib` Connectrix Fibre Channel Switch Trap MIB v4.0

Refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric Management Information Base Reference Manual* for more information.

Make sure that SNMP-FRAMEWORK-MIB and RFC1155-SMI are loaded before loading `v4_0FE.mib`.

Fabric Watch Profiles

The following Fabric Watch files are supported:

- `fw.workgroup.snmp` May 24, 2001
- `fw.workgroup.errlog` May 24, 2001
- `fw.enterprise.backbone.errlog` May 24, 2001
- `fw.enterprise.backbone.snmp` May 24, 2001
- `fw.debug.errlog` May 24, 2001

Refer to the *EMC Connectrix Departmental Switch DS-32B2 and ED-12000B Fabric Watch Reference Manual* for more information.

During a switch startup or switch reboot, the Fabric Watch daemon is one of the last processes to become active. Depending on the size of the fabric, Fabric Watch may take several minutes to complete its start up sequence. Before Fabric Watch is completely active, it will not be able to monitor events occurring in the fabric. During this time, the `switchStatusPolicyShow` command will show the default settings instead of any custom settings.

Getting Help

Switch serial number

The switch serial number is provided on the serial number label on the chassis. The serial number and bar code are printed on the label. The following example shows how the serial number appears:

```
FT00X0054E9
```

Switch License ID

Use the license ID string when obtaining license sets for your switch.

- ED-12000B and DS-32B2: The license ID of the chassis is provided by the `licenseidshow` command.
- DS-8, DS-16, and DS-16B2 switches: The switch license ID is provided by the `wwn` command (or by viewing the `switchshow` command output).

Password Security

To ensure security, you are prompted to change the root password during first login to the switch. This requires the default root password, which you can request from your support representative.

CAUTION

Root access should only be used by qualified personnel. Use of root access to monitor or manage the switch is not supported.

New Features and Enhancements

This section provides information on the new features and enhancements included in the Fabric OS v4.1.1.

High Availability

Additional high availability features include:

- Nondisruptive code activation on ED-12000B
- Nondisruptive failover between CPs (Control Processors) on the ED-12000B
- Additional background health monitoring of the STandby CP on the ED-12000B
- Managed hot swap procedure for the ED-12000B WWN / status card

Zoning

Zoning enhancements include:

- New commands for searching the Zoning database
- Improved performance
- More selective SCNs
  - SCNs are now sent only to devices in zones where there has been a status change among the online members of those zones

Web Tools

The Fabric View panel has been replaced with a switch explorer tree – an approach which allows Web Tools to handle larger fabrics more efficiently.

Ports

Disabling and enabling of ports and of entire switches may now be made persistent across reboots and power cycles.

Fabric Time Service

Improvements include:

- Synchronizes time among switches in the fabric
- Fabric time may be set from a CLI session or obtained from an external NTP server

fabricPrincipal command

A new fabricPrincipal command allows the administrator to give a switch preference in negotiating to become principal switch in a fabric. This can be useful in optimizing the efficiency of fabric configurations and management operations.

Fabric Watch

Improved reporting of port and switch uptime statistics have been added.

ED-12000B Domains

A maximum of sixteen ED-12000B domains are now supported with this release.

Requirements and Compatibility

This section includes requirements and compatibility for the ED-12000B and DS-32B2.

Hardware

The testing and qualification of solutions that include hardware from EMC and other vendors is an ongoing process. The most current list of qualified hardware solutions that attach safely to the ED-12000B and DS-32B2 can be found in the EMC Support Matrix (for more information, refer to: `http://powerlink.emc.com`). As additional support is added, the changes will be documented here first.

Fabric OS Switch Compatibility

Fabric OS version 4.1.1 can be installed and run on the Connectrix ED-12000B and DS-32B2 switches only. For this release of the product, the maximum fabric configuration is limited to sixteen domains with three hops between endpoints.

Standards Compliance

Fabric OS v4.1.1 is compliant with the following Fibre Channel standards:

- FC-AL ANSI X3.272.1996
- FC-AL-2 NCIT S 332: 1999
- FC-FLA NCIT S TR-20: 1998
- FC-GS-3 NCITS 348-2000 Rev 7.01
- FC-FG ANSI X3.289: 1996
- FC-PH ANSI X3.230: 1994
- FC-PH-2 ANSI X3.297: 1997
- FC-PH-3 ANSI X3.303: 1998
- FC-PLDA NCIT S TR-19: 1998
- FC-SW-2 Rev 5.3
- FC-VI Rev 1.61
- FC-MI, Rev 1.92
- FC-SB-2 Rev 2.1 (FICON Support)
- FC-BB Rev 4.7
- FC-FS Rev 1.7 (Still in draft)
- FC-BB-2 Rev 5.3 (Still in draft)
- IPFC RFC 2625
- FCP ANSI X3.269: 1996
- FCP-2 Rev 7

Firmware Licensing and Upgrading

Fabric OS v4.1.1 supports the following optional EMC software products:

- Performance Monitoring
- Web Tools
- Zoning
- Extended Fabric
- Fabric Watch
- ISL Trunking

The above products can be activated with the purchase of the applicable license key. Contact your switch supplier for software updates and maintenance releases. New switch firmware can be installed from any host running a Telnet session into the new switch.

E_Ports

E_Port connections between ED-12000B, DS-32B2, DS-8B, DS-16B, and DS-16B2, and other OEM versions are also supported. Check the EMC Support Matrix for minimum levels of firmware revisions.

Fabric Assist

EMC has no plans to support the Fabric Assist feature on the ED-12000B or DS-32B2.

Ficon

Ficon is not supported with this release.

Secure OS

Secure OS is not currently supported. Please check the EMC Support Matrix for the most up-to-date information.

ESN Manager

The ED-12000B and DS-32B2 are fully supported with ESN Manager 2.1. Zoning, discovery, and statistic polling of the ED-12000B and DS-32B2 with ESN Manager 2.0 or earlier versions, is not available with this release.

QuickLoop

QuickLoop will not be supported in the 4.x series of firmware.

EMC ControlCenter

Fabric OS 4.1.1 is not supported with EMC ControlCenter 5.1.1 SP2 or earlier versions. Please check the release notes for subsequent versions of EMC ControlCenter for updates.

Fabric Device Management Interface (FDMI)

This feature is not supported in this release.

Important Notes

Maximizing Fabric Availability During DS-32B2 Hot Code Activation

During code activation on a DS-32B2 running Fabric OS 4.1.1 or later, data keeps flowing between hosts and storage devices. However, fabric services are unavailable for a period of approximately 50-55 seconds. Possible disruption of the fabric can be minimized by ensuring that switches logically adjacent to the DS-32B2 (directly connected via an ISL) are running Fabric OS 2.6.1 or later, 3.1.1 or later, or 4.1.1 or later. More information is available in the *Firmware Download* section of the *Fabric OS Procedures* manual.

Microsoft Internet Explorer Issue

An issue has been identified with Microsoft Internet Explorer 5.0 and 5.5 running on Windows NT 4.0. The problem is as follows. Normally, when you launch a copy of the Switch Explorer applet, the left hand panel displays a tree of switches in your fabric. Clicking on a tree node will cause the right hand panels to refresh to the currently selected switch. However, under NT/4.0 and IE 5.0/5.5, the right hand panel will NOT update for the 2nd and subsequent instance of the Switch Explorer. Only the first instance works.

This issue has been identified and confirmed by Microsoft. For details, see the URL
`http://support.microsoft.com/default.aspx?scid=KB;en-us;242167&.`

Workaround: There are 2 workarounds for this:

- Always use a single instance of the SwitchExplorer on NT/4.0 and IE 5.0/5.5
- Install IE 6.0 SP1

Alternatively, it is possible that you can obtain a workaround directly from Microsoft for this problem. Please contact Microsoft support and supply them the information in the defect as described in the URL
`http://support.microsoft.com/default.aspx?scid=KB;en-us;242167&.`

Interpreting Ambient and Internal Temperatures

EMC Connectrix fabric switches are instrumented with temperature sensors to monitor the operating characteristics of the products and their environment. The following table explains how to interpret the various temperature readings that may be reported via Fabric OS v4 and monitored via the Fabric Watch optional licensed firmware product. All temperatures are degrees C.

Sensor	Minimum	Maximum	Comments
ED-12000B			
Blowers	0	40	Sensor on each blower measures inlet (ambient) air temperature.
Port Blades	0	74	Each port blade has its own temperature sensor.Warning at 75° C.; blade shutdown at 80° C.
CP Blades	0	74	Each CP blade has its own temperature sensor.Warning at 75° C.; CP will be faulted at 80° C.
DS-32B2			
Switch	0	69	Switch sends warning at internal temperature of 67° C. Switch begins 2 minute controlled shutdown at 69° C.

Other Important Notes

Area	Description
Ethernet Port IP addresses	When an ED-12000B fails over to its Standby CP for any reason, the IP addresses for the two logical switches move to that CP blade's Ethernet port. This may cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, since the association between the IP addresses and MAC addresses has changed.
Fabric OS CLI commands, Failover and Port disable	Changing port configurations during a failover might cause ports to be in a disabled state. Reissue the command after the failover is complete to bring the port online.
Fabric OS Commands	**Problem:** Under the root account, issuing Fabric OS commands in parallel through scripts could cause the Kernel task to consume excessive memory. **Solution:** When using scripts to issue Fabric OS commands, it is always a good practice to wait for the command to finish before issuing another command.
Fabric OS Commands	The commands moredisable and moreenable were added to the Fabric OS.
Fabric OS Switch Beaconing	Switch beaconing is not preserved across a failover. If you start beaconing, a failover will cause all lights to stop flashing. **Solution:** If this occurs, reissue the command to resume switch beaconing.
Fabric OS, Switch reboot and Blade Repair	**Problem:** Switch reboot will fail in the ED-12000B, if there are faulty port blades. **CAUTION:** Verify all blades are in working order before performing a switch reboot. Switch reboot is meant to be issued after all repairs are complete. If you do a switch reboot and find a faulty blade, remove the blade and reboot will continue. **Solution:** Identify and remove the faulty blade using the slotshow command to reboot successfully.

Area	Description
Fabric routing, Fabric Manager: domain overlap	Issuing a configdefault followed by reboot or switch disable/enable will cause the fabric to segment due to possible domain overlap. **Solution:** Therefore, before rebooting the Fabric, ensure all switches are properly configured to avoid domain overlap between the logical switches.
Fabric Device Management Interface (FDMI)	An HBA will be allowed to register even though the originating port is not in the HBA's registered port list. This is intended behavior included in order to test error cases.
Firmware Download	Please review the Firmware Download section of the Fabric OS Procedures guide before upgrading your firmware.
Firmware Download	**Problem:** During a firmware download, rebooting or power cycling the CPs could cause the compact flash to be corrupted. **CAUTION:** Do not attempt to power off the CP board during Firmware Download to avoid high risk of potentially corrupting your flash.
HA switch reboot failure	When a switch reboot or a failover occurs before POST is complete, the HA resynchronization will be disrupted. HA will not resynchronize until POST completes. **CAUTION:** Allow POST to complete before performing a switch reboot or failover to avoid disruptive failover.
IP addresses	**CAUTION:** Do not set a switch or CP IP address for the Ethernet interface to 0.0.0.0.
License removal	When a user removes a license from the switch, the feature is not disabled until the switch is rebooted or a switch disable/enable is performed.
LTO 2 Tape Drive Support	When using the LTO 2 Tape Drive, the user must perform the following command on both Fabric OS 3.x and 4.x: `switch> portcfggport port#` *where drive is plugged into* This will allow the tape drive to function in point to point mode rather than in loop.

Area	Description
OS - Hardware	Bringing up port blades during a failover could cause the port cards to come up in a disabled state. This is a rare occurrence, and when this happens, redo the port blade bringup after the failover on the ED-12000B.
Security	If HTTP_Policy is empty you will not be able to log in and will receive a "Page not found" error. This is expected behavior for this policy.
Security, FCC list	Adding switches onto the FCC list does not automatically join the switches in a secure fabric. Add the switches to the FCC list and either reset the E-ports or perform a switch disable and enable for the switches to join.
Security, PKICERT utility	Before using the PKICERT utility to prepare a CSR, please ensure that there are no spaces in the switchnames of any switches in the fabric. The website that processes the CSRs and generates the digital certificates does not accept switchnames containing spaces, and any CSRs that do not conform to this requirement will be rejected.
Security, SLAP fail counter and 2 switches	The SLAP counter is designed to work when all the switches in the fabric are in secure mode. All the switches in the fabric must be in secure mode for accurate SLAP statistics.
Security, SSH login	To properly connect SSH login, wait for sec mode to complete before rebooting or doing HA failover on the ED-12000B. If Sec mode is enabled and a reboot occurs before Sec mode completes, SSH login will not connect and will go to the wrong MAC address because the active CP would change after a HA failover.
Security: Empty policies	**CAUTION:** If telnet, API, and serial port access policies are empty, the user will not be able to talk to the switch. **Solution:** Contact switch provider for the recovery procedure.
Security: Error counter	The Telnet security error counter will count each violation as 1 plus any auto retries the telnet software executes.
Security: Secure mode	When in Secure mode, if you upgrade from Fabric OS version 4.0 to 4.1, then downgrade to Fabric OS version 4.0, and upgrade back to Fabric OS version 4.1, the system prompt will ask the user to reset the secure mode password.

Area	Description
Security: Secure mode, passwd telnet	**CAUTION:** Using the passwd telnet command in Secure Mode to change the password results in all sessions using that password to be logged out including the session that changed the session. This is expected behavior. The session will terminate if you change the password in secure mode.
Web Tools and CLI commands	If you use Web Tools to change the switchName, the ED-12000B telnet console prompt will not update to the new name until a new telnet window is opened.
Web tools, Java bug	**Problem:** If a dialog box is displayed from the switch admin window of the Web Tools and the user selects another dialog box from Web Tools, this causes a windows display error. This is a known defect in Java 1.3 documented at www.java.sun.com, bug ID 4763605. To avoid the display error, open only one dialog box at a time or launch another switch admin session in a separate window.
WWN card FRU repair	**Problem:** If an HA failover or power cycle occurs during a FRU on the WWN card, the SilkWorm 12000 will become non-operational. **CAUTION:** When performing a FRU on a WWN card, complete the FRU procedure before attempting an HA failover or power cycling the chassis.

Area	Description
Zoning	To use Zoning in a non-RCS (Reliable Commit Service) mode fabric, that is, in a fabric containing switches with firmware version other than v2.6.x, v3.1 and v4.1, it is recommended that all appropriate Zoning licenses are installed on all the switches in the fabric before attempting to bring a switch in to the fabric. Furthermore, if the Zoning license is to be removed, the user must make sure it is re-installed back properly on the affected switch before attempting cfgenable zoning operation. Failure to follow these steps can cause inconsistency of Zoning configuration on the affected switches should a zoning operation be attempted from a remote switch in the fabric. On the affected switches an error message will appear on the console or telnet session (can also be seen by doing errShow, errDump) indicating that zoning license was missing.
Zoning	**Problem:** Domain 0 in a zoning configuration file is illegal but was not previously enforced. Prior to upgrading a switch to 4.1, please ensure that the fabric's zoning configuration does not contain the Domain ID 0 used for zoning. This is specific only to 4.x switches.

Limitations

Fabric Watch

During a switch startup or switch reboot, the Fabric Watch daemon is one of the last processes to become active. Depending on the size of the fabric, Fabric Watch might take several minutes to complete its start up sequence. Before Fabric Watch is completely active, it will not be able to monitor events occurring in the fabric. During this time, the `switchstatuspolicyshow` command will show the default settings instead of any custom settings.

Trunking

Trunking is only supported for normal E_Ports (referred to as L0 in the portcfglongdistance command) up to 5 km at the full speed permitted by the link. For information about these modes and Extended Fabrics in general, refer to the *EMC Connectrix B Series Extended Fabrics User Guide*.

QuickLoop

QuickLoop is not supported on the ED-12000B in either its original hub emulation mode, or in Fabric Assist mode. This means that direct attachment of private hosts to the ED-12000B is not supported.

ESN Manager, EMC ControlCenter, and Passwords

Because of new security features introduced in Fabric OS version 2.6.x, 3.1.x, and 4.1x, ESN Manager and EMC ControlCenter will not be able to communicate with the switch if the default passwords are not changed immediately after an upgrade to 2.6.x, 3.1.x, or 4.1x.

DS-8B and DS-16B Scalability Limits

Exhaustive testing has demonstrated that DS-8B and DS-16B switches should not be deployed in fabrics whose size exceeds 500 user ports (device ports). Such switches will not be supported in fabrics that exceed this size, regardless of Fabric OS version.

Port Swapping

Swapped ports do not get saved as part of a config upload. In addition, when Fabric Watch detects errors on swapped ports, the wrong area number will be reported.

Gateway Compatability

Gateway Compatibility (R_RDY) is not currently supported.

Documentation Issues

Numerous Documents

In numerous documents the sentence , "The default administration logon is `admin` and the default password is `password`" was changed to read,"The default administration logon is admin."

The default password was erroneously deleted and should have remained as part of the sentence. The default password *is* `password`.

DS-32B2 Hardware Reference Manual

The following statement should be added to the Port Status LED information for when the port status is "offline" in Table 3-1 "Port Side LED Patterns During Normal Operation".

"When a Port Status LED indicator light is off, another possible hardware status is offline."

Quickstart Guide for the Model ED-12000B

The EMC Connectrix Enterprise Director Model ED-12000B can be installed in the following ways:

- Set up as a stand-alone unit on a flat surface.
- Installed in a 19-inch EIA (Electronic Industries Association) cabinet, using the 14U Rack Mount Kit provided with the ED-12000B (detailed instructions included with kit). Up to two ED-12000Bs can be installed in a 42U EIA cabinet, and they must be installed in the lowest 32U of the rack.

Leave at least one U between the switch and any other device in the rack.

The instructions in this quickstart guide for the Model ED-12000B are written with the following assumptions:

- The *service aisle* refers to the aisle into which exhaust air is released.
- The chassis is installed with the port side facing the service aisle.

This guide provides the following information:

Installation Considerations and Safety Guidelines

It is recommended that only EMC personnel install the ED-12000B. It is not a customer-installable product.

WARNING

A fully populated ED-12000B weighs approximately 250 pounds (275 pounds including the rail kit) and requires a minimum of two people and a hydraulic or assisted lift to install it. Before installing, verify that the additional weight of the chassis does not exceed the cabinet's weight limits or unbalance the cabinet, including when some of the cards or power supplies are partially extended out of the chassis.

CAUTION

To ensure adequate cooling, install the chassis with the port side facing the aisle into which exhaust air is released (usually called the *service aisle*). This prevents the fans from pulling in heated exhaust air.

The following steps are required to ensure correct installation and operation:

- Ensure the space in the EIA cabinet is 14U high, 30 inches deep, and 19 inches wide, with a minimum distance of 28.25 inches between the front and back rails.
- Verify that the additional weight of the chassis does not exceed the cabinet's weight limits.
- Plan for cable management before installing the chassis. Cables can be managed in a variety of ways, such as by routing cables below the chassis, to either side of the chassis, through cable channels on the sides of the cabinet, or by using patch panels.
- Ensure that two dedicated electrical branch circuits with the following characteristics are available:
  - 200 to 240 VAC, 50-60 Hertz (refer to the *EMC Connectrix Enterprise Director Model ED-12000B Hardware Reference Manual* for additional electrical specifications)
  - Protected by a circuit breaker in accordance with local electrical codes
  - Supply circuit, line fusing, and wire size that are adequate according to the electrical rating on the chassis nameplate
  - Grounded outlets installed by a licensed electrician and compatible with the power cords
- Ensure that all equipment 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.
- Ensure the ED-12000B has access to a minimum airflow of 350 cubic feet per minute.
- Ensure the air temperature at the blower inlet does not exceed 104° F (40° C) during operation.

Items Included with the EMC Connectrix Enterprise Director Model ED-12000B

The following items are included with the standard shipment of the EMC Connectrix Enterprise Director Model ED-12000B:

- The EMC Connectrix Enterprise Director Model ED-12000B, populated with:
  - Eight 16-port cards, for a total of 128 ports configured into two 64-port domains
  - Four power supplies
  - Three blower assemblies
- One Accessory Kit containing the following items:
  - Two AC power cords
  - ESD grounding strap
  - Power cord retainer
  - One 10-foot (3.05 meters) RS-232 serial cable, with an RJ-45 connector/adapter on the end of the cable
  - Eight fibre-optic cable guides
  - Rack mount kit

Unpacking the ED-12000B

This procedure requires a 1/2-inch socket wrench to remove the pallet bolts.

To unpack the ED-12000B:

1. Open the shipping crate and remove the packing foam and antistatic plastic.

   To open one of the hinges on the crate, pull the handle out and turn counter-clockwise (to left); and then slide open.

2. Unscrew the four bolts holding the ED-12000B to the pallet (see Figure 1), and remove the brackets.

CAUTION

Remove the chassis door before moving the chassis.

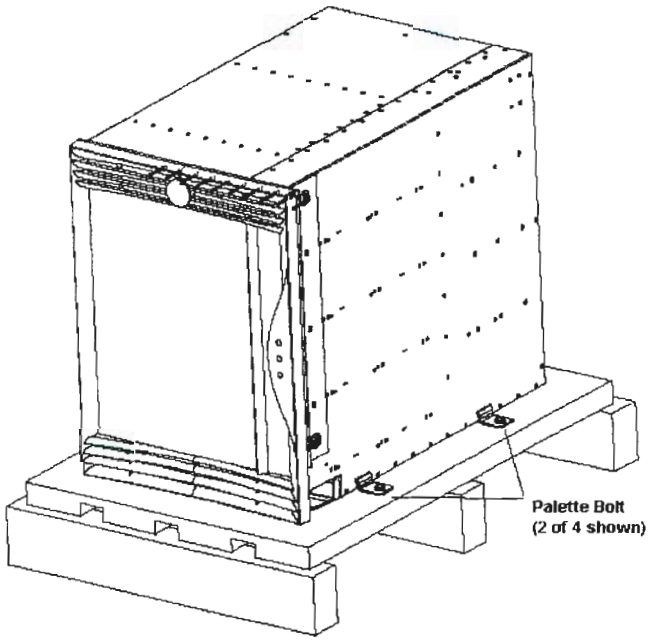


Figure 1 **EMC Connectrix Enterprise Director Model ED-12000B on its Shipping Pallet**

3. Remove the chassis door from the chassis.
   a. Open the door to a 90-degree angle.
   b. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge.
   c. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge, supporting the door to prevent it from falling.

Setting Up the ED-12000B As a Stand-alone Unit

If the ED-12000B is to be set up as a stand-alone unit, it must be placed on a stable, flat surface, with the blower side of the chassis having access to cool air. EMC recommends orienting it so that the port side faces the service aisle.

To reinstall the door once the chassis is in place:

1. Ensure that the spring-loaded pins on both door hinges are retracted (push levers into notches).

2. Align the door hinges with the chassis portion of the hinges.
3. Release the pins by pushing the levers out of the notches.

Providing Power to the ED-12000B

To provide power to the ED-12000B, follow the steps below.

1. Connect the power cords to a 200 to 240 VAC, 50-60 Hz power source.
2. Connect the AC power cord retainer to the chassis (see Figure 2):
   a. Position a retainer over an AC power connector, oriented as shown in Figure 2, hooking the retainer tabs over the two screws on either side of the power connector. Tighten both screws.
   b. Loosen the adjusting screw to allow the power cord to fit into the retainer.
   c. Repeat steps 2a and 2b for the other retainer.

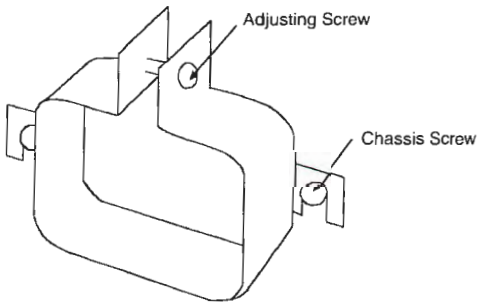


Figure 2 Power Cord Retainer

3. Connect the power cords to the power connectors on the ED-12000B, inserting them through the retainers. The power cords are designed with right and left bends to facilitate cord management. Ensure each cord has a minimum service loop of 6 inches at the connection to the switch, and is not exposed to stress.
4. Tighten the adjusting screws on both retainers until the power cords cannot be disconnected.
5. Flip both AC switches to 1. The AC switches illuminate green.

The ED-12000B automatically performs POST (power-on self test) by default each time it is powered on. POST takes a minimum of three minutes, and is complete when indicator light activity returns to standard state. For information about indicator light patterns, refer to the *EMC Connectrix Enterprise Director Model ED-12000B Hardware Reference Manual.*

CAUTION

Do not connect the switch to the network until the IP address is correctly set. For instructions on how to configure the IP address, refer to the *EMC Connectrix Enterprise Director Model ED-12000B Hardware Reference Manual.*

QuickStart Guide for the Model DS-32B2

This section provides the following information:

- Installation and Safety Considerations
- Items included with DS-32B2
- Setting up the DS-32B2 as a stand-alone unit
- Providing power to the DS-32B2

Cabinet mounting and configuration instructions are provided in the *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*, available on the EMC Documentation CD-ROM. Cabinet mounting instructions are also provided in the *Slide Rack Mount Kit Installation Procedure*, included with the Slide Rack Mount Kit.

Installation and Safety Considerations

You can install the DS-32B2 as a stand-alone unit on a flat surface or in an Electronic Industries Association (EIA) cabinet using the Slide Rack Mount Kit provided with the switch.

For successful installation and operation of the switch:

- Ensure the following electrical requirements are met:
  - Primary AC Input 100-240 VAC (the switch auto-senses input voltage), 47-63 HZ.
  - Correctly wired primary outlet, with circuit protected by a circuit breaker and grounded in accordance with local electrical codes.
  - Adequate supply circuit, line fusing, and wire size, as specified by electrical rating on switch nameplate
- To ensure adequate cooling, install switch with non-port side, which contains air intake vents, facing cool-air aisle.
- Verify a minimum of 47 cubic feet/minute (79.8 cubic meters/hour) of air flow is available to air intake vents on non-port side of the switch.
- Verify that the ambient air temperature does not exceed 40° Celsius (104° Farenheit) while the switch is operating.

- If installing the switch in a cabinet:
  - The cabinet must be a standard EIA cabinet.
  - Plan a cabinet space that is 1.5 rack units high (2.6 inches; 6.7 cm), 19 inches (48.3 cm) wide, and at least 23 inches (68.6 cm) deep.
  - Ground all equipment through a reliable branch circuit connection and maintain ground at all times. Do not rely on a secondary connection to a branch circuit (such as a power strip).
  - Ensure that airflow and temperature requirements are met on an ongoing basis, particularly if the switch is installed in a closed or multi-rack assembly.
  - Verify that the additional weight of the switch does not exceed the cabinet's weight limits or unbalance the cabinet in any way.
  - Secure the cabinet to insure stability in case of unexpected movement.

Items Included With the DS-32B2

The following items are included with the standard shipment of the DS-32B2:

- The DS-32B2 switch, containing three fan assemblies, two power supplies, 32 SFPs (small form factor pluggable) transceivers
- Slide Rack Mount Kit, with installation instructions included
- One accessory kit, containing the following items:
  - The *DS-32B2 QuickStart Guide* (this document)
  - The EMC Documentation CD-ROM
  - (optional)
  - Rubber mounting feet
  - Two grounded 10 foot (approximately 3 meter) country-specific power cords
  - One serial cable, 10 ft. (3.0 m) long, which can be converted from a DB-9 serial cable to an RJ-45-style serial cable by removing the adapter on the end of the cable

Setting Up the DS-32B2 as a Stand-Alone Unit

1. Unpack the DS-32B2, and verify all ordered items are present.
2. Clean the four corner depressions on the bottom of the switch and place a rubber foot in each depression.
   This helps prevent the switch from accidentally sliding off the supporting surface.
3. Place the switch on a stable, flat surface.

Providing Power to the DS-32B2

Power is supplied to the switch as soon as the first power supply is connected and powered on.

1. Connect the power cords to both power supplies and to power sources. To protect against AC failure, connect the power cords to outlets on separate circuits.
   Ensure that the cords have a minimum service loop of 6 inches available at the connection to the switch, and are routed to avoid stress.
2. Power on the power supplies by flipping both AC switches to `1`. The power supply LED lights up green and the switch begins running POST. The switch requires a minimum of three minutes to boot and complete POST.

CAUTION

Do not connect the switch to the network until the IP address is correctly set. For instructions on setting the IP address, refer to the *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*, provided on the EMC Documentation CD-ROM.

Defect Lists

This section contains a list of defects:

- Outstanding Software Defects
- Fixed Defects between v4.0.2a and v4.1.1

Software Defects in v4.1.1

The following table lists outstanding software defects in the Fabric OS v4.1.1. release.

Table 1 Software Defects in Fabric OS v4.1.1 Release

Defect ID	Severity	Summary
000025878	High	**Summary:** VE: Burnin failed on the 3rd run. **Symptom:** While running burning, port becomes online before initialization is done and it results in txdpath TIME-OUT errors. **Customer Impact:** This is a very difficult timing condition to reproduce the error. A solution is being planned for a release after 4.1.1.
000025890	High	**Summary:** Switch Status Marked As Health When CF (compact Flash) 100% Full With Write Errors. **Symptom:** Switch status does not reflect the down graded potentially critical condition of the switch. **Customer Impact:** Request to update health status when compact flash is full will be delivered in a release following 4.1.1
000025892	High	**Summary:** Webtools Failed To Log Level 1 Kernel Software Watch Dog Errors. **Symptom:** CLI command: errorshow has KSWD event listed, but WebTools does not. **Customer Impact:** Event notification will be added in a release following 4.1.1

Table 1 Software Defects in Fabric OS v4.1.1 Release (continued)

000025910	High	**Summary:** After changing Ethernet IP address from CLI or from WT, can not launch WT with new IP address. **Symptom:** Web Tools can not be launched with new IP address. **Customer Impact:** Issue is being investigated, and will be targeted for a future release of Fabric OS.
000025948	High	**Summary:** 147698 Switch Failed To Generate Any Event, KSWD, Core Dump Notification After RPCD Issue. **Symptom:** Errshow contains no event notification regarding the failed status of the switch. **Customer Impact:** The message produced from this error condition will be improved to be more recognizable and to provide proper guidance. This issue will be targeted for delivery in a future release of the Fabric OS.
000025949	High	**Summary:** 147692 v4.1.1_rc2 Firmware Download Hangs Switch After Critical SYSC-ERROR Seen. **Symptom:** Switch lost connectivity, services not able to support commands, firmware no able to commit until rebooted. **Customer Impact:** Switch was unable to close all open processes due to an error condition created prior to the firmware download. Improvements to the error detection and reporting during the hot code load are currently under development to address this issue for release in a future version of the Fabric OS.
000025679	Medium	**Summary:** Right after activated SCC policy, retrieve sec policy through API will fail. **Symptom:** Retrieving the sec policy via the Fabric Access API, immediately after activating a new SCC policy will cause the retrieval command to fail. **Comment:** The fix for this defect is currently under test.
000025783	Medium	**Summary:** portstats do not match portperfshow. **Symptom:** The portstats output from the Fabric Access API does not match the output from the CLI portPerfShow. **Customer Impact:** Issue is being investigated, and will be targeted for a future release of Fabric OS.

Table 1 Software Defects in Fabric OS v4.1.1 Release (continued)

000025854	Medium	**Summary:** Security Admin returns Error -55 after removing/adding members and Activate FCS Policy. **Symptom:** In a large fabric containing over 26 switches. When using the Fabric Access API to remove multiple FCS members without first performing a save operation, an error is returned. **Customer Impact:** The fix for this defect will be considered for a release following 4.1.1. This error condition does not happen when using the CLI, or when performed after a save operation from the API.
000025889	Medium	**Summary:** Receiving "hwclock: Could not update file with the clock adjustment parameters (/etc/adjtime) in it, errno=28: No space left on device." message and after a hafailover, the switch did not come up. **Symptom:** "No space left" message is printed in the console and after a hafailover, the CP failed to mount root directory and the switch did not come up. **Customer Impact:** Improvements to monitor compact flash usage will be made in a release after 4.1.1
000025895	Medium	**Summary:** No Event Generated For CF(compact flash full 100% capacity error). **Symptom:** When the compact flash was filled 100% capacity no event was generated to alert the user of this condition. **Customer Impact:** Request to create a new monitor to detect compact flash capacity will be considered for a release after 4.1.1
000025896	Medium	**Summary:** Save Core #2 Option Requires Full Pathing To FTP Directory From Root. **Symptom:** FTP login configuration places users in a directory, should not have to list it for Savecore utility. **Customer Impact:** Fix will be considered for release following 4.1.1.

Table 1 Software Defects in Fabric OS v4.1.1 Release (continued)

000025922	Medium	**Summary:** emd failed to refresh SWD after doing bladedisable/hafailover followed by firmwaredownload 5 hours later. **Symptom:** SWD error observed on a firmware download after running a bladedisable/hafailover stress test. **Solution:** The fix is in zn_native_ha.c@@/main/18.I will merge the fix into Meteor branch. **Customer Impact:** Issue is being investigated, and will be targeted for a future release of Fabric OS.
000025926	Medium	**Summary:** Switch dumps core when run HA stress testing, ASSERT - Failed expression: (portp = (fabobj_port_user(handle))) != NULL, file = switch_ha.c, line = 1868, kernel mode. **Symptom:** Fabric Access API stress test case involving FSPF data access and ha failovers. **Customer Impact:** This defect is being investigated, but is currently not reproducible. This defect is currently in a re-test state.
000025939	Medium	**Summary:** Spinfab command failed while running on two Ulysses slots. **Symptom:** The command "Spinfab" failed while Spinfab was running on slot2 and slot4. The error message was "No Longer Transmitting, FTX Counter Stuck At xx". **Customer Impact**: Issue is being investigated, and will be targeted for a future release of Fabric OS.
000025989	Medium	**Summary:** Webtools shows incorrect "Current" value on the smart sfp. **Symptom:** The output of sfpshow from the CLI and from Webtools is different. Web Tools is displaying an incorrect value for the current value on smart SFPs. **Customer Impact:** This issue will be targeted for delivery in the next maintenance release.

Table 1 Software Defects in Fabric OS v4.1.1 Release (continued)

000026016	Medium	**Summary:** sw0: BLOOM 4: S4,P49(14): Warn: bloomCheckBuf: invalid frontend desired buffers: 54, max_bufs 27, blm_type 0x36. **Symptom:** Test consisting of configuring all ports within a quad as long distance ports, thus causing an over subscription of buffers. Resetting all but one of the ports back to normal distance, and then causing an hafailover. The ports that were at one time oversubscribed will cause an error message to be displayed indicating that the desired number of buffers could not be applied. **Customer Impact:** This issue will be targeted for delivery in the next maintenance release.
000026004	Low	**Summary:** Help for portloginshow is not correct. **Symptom:** When you display the help file for the command portloginshow, the information displayed is incorrect. **Customer Impact:** A fix would be implemented in the next maintenance release following 4.1.1.
000025808	Low	**Summary:** In Web tools Event log, clicking on time doesn't sort it by the time and no year included in date. **Symptom:** When events in eventlog span a year boundary, the events may not be listed in the proper order. **Customer Impact:** A fix would be implemented in the next maintenance release following 4.1.1.

Software Defects in Previous Releases

This table contains defects opened against a previous Fabric OS releases which are being deferred to a future release.

Table 2 Software Defects in Previous Releases

Defect ID	Severity	Summary
000020911	High	**Summary:** IDIDMode reporting should reflect the status of fabric wide IDIDmode. **Symptom:** Two independent switches, or fabrics, with security enabled but ficonmode disabled on one of them, are allowed to merge without reporting to the attached FICON Host that IDID is not guaranteed in the fabric. **Customer Impact:** This defect will only be seen in a cascaded FICON environment.
000023464	High	**Summary:** Zoning script causes active CP to run out of memory (kills all zoned processes). **Symptom:** Overnight stress test of zoning caused the zoning task to be killed by the Linux memory killer. **Customer Impact**: This is Stress to Fail test case. Running under standard stress conditions could not reproduce the error in a 48 hour test run.
000023630	High	**Summary:** Host Detected IC03 Link Incidents during reboot, fastReboot and haReboot process. **Symptom:** The FICON mainframe detected two link incidents during a non-error, user-requested CP reboot process.Workaround: Use switchreboot as an alternative. No Link Incidents are generated as a result of switchreboot. **Customer Impact:** This defect will only be seen in a FICON environment.

Table 2 Software Defects in Previous Releases (continued)

000024431	High	**Summary:** Switch (active CP) reset when switchdisable/enable script running. **Symptom:** Overnight stress test which involves issuing simultaneous switchdisable commands to all 34 switches of a core-edge fabric, followed by simultaneous switchenable commands to all 34 switches. **Customer Impact:** This is a Stress to Fail test case that requires running for long periods of time before encountering the CP reset on one of the core switches. The switch performed a fail-over, and the fabric continued to run without disruption.
000024653	High	**Summary:** After running continuous loops of switchblade related commands, SYSCTRLD: received an invalid token: show up on console and ASSERT - Failed expression: em_waitfor_sysctrl(pFruObject, TRUE) == SUCCESS **Symptom:** Stress test in which multiple concurrent failure events are simulated in a rapid sequence. **Customer Impact**: Stress to Fail test that is designed to overload the CPU processing power of the switch. **Probability:** Low
000024982	High	**Summary:** Establishing 5 sessions each to 2 4.1 switches and calling GetAllObjectsBySession core dumps msd and returning objects with -209 & -86 when fabric is stable. **Symptom:** Using the Fabric Access API to retrieve the current FICON mode setting via ten concurrent sessions (five on each switch) caused a core dump of the Management Server process. **Comment:** The fix for this defect is currently under test.
000025179	High	**Summary:** When doing AddAttribute to change Switch IP Address to "0.0.0.0", Switch Panics and Dumps core. Switch reboots continuously. **Symptom:** Setting switch IP address to 0.0.0.0 during an SNMP or API management session caused the switch to panic. **Customer Impact:** This action would clearly disrupt any management session, and should never be done.

Table 2 Software Defects in Previous Releases (continued)

000025331	High	**Summary:** Modifying switch and CP IP addresses caused a telnet hang.Symptom: Changing the switch IP address before changing the CP IP address will cause the CP IP address to become inaccessible on a subsequent attempt to set the switch IP address. **Workaround:** When both CP and switch IP addresses need to be changed: set the CP IP address first and then the switch IP address. When only a switch IP address needs to be changed, set the CP IP address first (keeping the current value) and then the switch IP address to its new value. When only a CP IP address needs to be changed, there is no problem; just change the CP IP address. If a customer gets into this scenario, telnet into the switch and set the CP IP address again, accepting the default values. **Customer Impact:** This behavior is identical to how the code works in 4.0.2. There is a well-documented workaround.
000025474	High	**Summary:** After fastbooting standby CP of the primary FCS, doing secfcsfailover before HA is in sync results in old primary FCS switch's active CP panicking. **Symptom:** This is multiple failure test case, on which first the standby CP of the primary FCS switch is issued a fastboot and then prior to the HA state achieving synchronization, a 'secfcsfailover' command is issued from a standby FCS switch. The old primary FCS switch is segmented out of the fabric.Workaround: Issue switchdisable, switchenable to the segmented switch to cause it to rejoin the fabric. **Comment:** The fix for this defect is currently under test.
000025718	High	**Summary:** slotPowerOff causes Ficon host to detect and report IC03 Link Incidents. **Symptom:** This defect will result in a call home and subsequent replacement of a FRU when the slotpoweroff command is executed. **Customer Impact:** The fix is being addressed in a Fabric OS 4.2 release.

Table 2 Software Defects in Previous Releases (continued)

000025747	High	**Summary:** Message "Oops: kernel access of bad area, sig: 11" shows up and switch reset. **Symptom:** Stress test involving a 34-switch fabric, on which one of the core switches is constantly being issued the hafailover command. Simultaneously, one of the edge switches is constantly having its zoning configuration updated. **Comment:** The fix for this defect is currently under test.
000021352	Medium	**Summary:** fruHistoryTrap is not generated or is not generated properly. **Symptom:** SNMP FRU history trap is not always generated as expected. **Customer Impact:** With the addition of the Managed WWN card Hot swap, the FRU trap mechanism does not always catch the fact that the WWN card has been replaced. However, this is not like a blower which can be hot swapped without the administrator knowing about it. Hot swap of the WWN card REQUIRES active participation by the administrator.
000021881	Medium	**Summary:** No trap generated when firmwareDownload completes. **Symptom:** No SNMP trap is generated when a firmwareDownload completes. **Customer Impact:** This is a request to create a new type of SNMP trap mechanism to inform the SNMP agent upon the completion of a Hot Code Activation. This new mechanism has been implemented and verified for SW12000 systems in Fabric OS 4.1.1; however, the solution for non-bladed platforms will be targeted at a release after 4.1.1.
000024542	Medium	**Summary:** No log message is generated when one CP resets the other CP. **Solution:** This message was removed in order to fix Defect 25094.Customer Impact: There will be no message printed when one CP resets the other.
000024679	Medium	**Summary:** FICON can be enabled on a 'disabled' switch which has security 'disabled'... **Comment:** The fix for this defect is currently under test.

Table 2 Software Defects in Previous Releases (continued)

000024769	Medium	**Summary:** REG: EVT_TC_154 : When trunk port is disabled on 4.1 proxy switch, API is receiving an EV_STATE_CHANGE event 2 times. **Symptom:** Fabric Access API test case in which a trunking port is disabled, but the disable event is being reported twice via the API. **Customer Impact:** This issue will only be seen when using the Fabric Access API. The two events being reported are "Trunking port down" followed by "Port Down". If the user did not realize they were disabling a trunking port, then the two status changes could be interpreted as confusing. This behavior will be documented in the Fabric Access API documentation.
000024773	Medium	**Summary:** When 4.1 Proxy Switch is disabled, switch generates lot of events saying Trunk Ports are disabled. But API is not receiving any such events. **Symptom:** Fabric Access API test case that causes Trunking port events to be reported to the console, but there are no events reported via the API. **Customer Impact:** This Trunking port console messages are the result of an end user request to have printed messages on the console port. These are not error log events, and thus are not being reported via the API. This is an RFE that is being considered for a future release.
000024892	Medium	**Summary:** No sequence open on the tx queue sw1: FCPH 0. This child defect of 22412 by using Xyratex. **Symptom:** Stress test case in which 4 loops of 120 devices each are simulated using test equipment. These four loops are further connected to all 4 ports of one quad within the ASIC. All four loop simulators then stress the system by simultaneously resetting their loops and causing loop initialization issues. **Customer Impact:** This is a Stress To Fail test that requires the use of fabric testing simulators.

Table 2 Software Defects in Previous Releases (continued)

000024975	Medium	**Summary:** when configdownload succeeded on zoneDB but failed on sec policy, primary fails to propagate zoneDB to fabric. **Symptom:** When performing a configDownload that modifies both the zoning DB and the security DB, an error within the security DB will prevent the zoning DB from being activated in the fabric, but it will not prevent it from being loaded into the flash memory. **Workaround:** Correct your mistake in the Security section of the configuration file and repeat the configDownload. Do NOT reboot the FCS prior to correcting the configuration file. **Customer Impact:** This situation will only happen when both zoning and security DB are modified, and an error is injected into the security DB config. The root cause is well understood; however, the complexity of the required modifications to the configDownload code would have introduced significant risk to the program.
000025156	Medium	**Summary:** Error related to blade- 9 and 10 were logged to switch-0 error log instead of switch-1 error log. **Symptom:** A faulty blade inserted into slot 9 or 10 of the switch was producing the appropriate error messages, but they were being logged under switch 0's error log instead of switch 1 as expected. **Customer Impact:** The logging mechanism prior to the switch being fully online is to log all errors to switch 0's error log. This is an identical mechanism to 4.0.0 and 4.0.2.
000025216	Medium	**Summary:** The time stamp for firmware download from Fabric Manager/Webtools is off by 8 hours compared to time on the switch. **Symptom:** Users who attempt to upgrade switch firmware from Fabric Manager or Webtools, will see a time difference of 8 hours. **Customer Impact**: There is no operational impact due to this defect.

Table 2 Software Defects in Previous Releases (continued)

000025259	Medium	**Summary:** 4.1 switch panic and dump core during switchreboot. **Symptom:** A switch panic was observed during a Fabric Access API test run. **Customer Impact:** This defect cannot be recreated and has not been seen since it was first observed. The core dump has provided the root cause of the problem and an architectural solution is currently under investigation for a future release.
000025297	Medium	**Summary:** "tsd" core dump on SW3900 switch interrupted the time synchronization with Primary FCS switch. **Symptom:** When a switch reboot or panic takes place when a Time Service update is in progress, the time server failed the synchronization with the Primary FCS switch. **Customer Impact:** The time service synchronization will fail only if a reboot or panic is observed concurrently with the synchronization. Re-issuing the time service command will cause the synchronization to take place. **Probability:** Low
000025401	Medium	**Summary:** Swap 1 G and 2 G HBAs and haFailover, sometimes the PRLI ACC frame got dropped and then host can't see target. **Symptom:** swap 1G and 2G HBA (both Emulex) using Apcon and do haFailover immediately, sometimes the PRLI ACC frame get dropped and Host can't see target. **Comment:** The fix for this defect is currently under test.
000025494	Medium	**Summary:** Web Tools display of segmented trunk ports. **Symptom:** In the Web Tools display, when a trunk group is segmented, only the trunk master is shown with a blinking light indicating an error. The other links in the trunk continue to be shown with a solid green light, suggesting no error. **Customer Impact:** The fix for this defect will be considered for a release following 4.1.1

Table 2 Software Defects in Previous Releases (continued)

000025534	Medium	**Summary:** SwitchCfgTrunk leaves ports disabled if a long distance port is configured on the switch. **Symptom:** Activating Trunking at the switch level (switchCfgTrunk) when a long-distance port is currently configured causes the error message "No Trunking support of long distance port" to be displayed, which is correct. However, other trunk ports are then left in a disabled state. **Workaround:** There are 2 ways to avoid this issue: 1. Using command port portcfgtrunkport to enable the trunk for each port (recommended) 2. Disable long distance port before issue switchcfgtrunk. **Customer Impact:** This defect will be deferred for consideration in a future release.
000025543	Medium	**Summary:** Step 9 of Firmwaredownload Completes With Error: CP1: Standby cp failed to reboot. **Symptom:** Standby CP failed to reboot when upgrading to 4.1.0_rc1; both CPs restore from secondary partition to correct itself. **Workaround:** Turning off POST prior to upgrading the FW from 4.0.2 to 4.1.0 should ensure that this error message is not displayed. **Customer Impact:** The firmwareDownload failed at the auto-Commit stage, however the firmwareDownload actually completed. A manual reboot of the machine resulted in the SW 12000 running properly with Fabric OS 4.1.0.

Table 2 Software Defects in Previous Releases (continued)

000025580	Medium	**Summary:** Able to reset version time stamp when logged in as "user". **Customer Impact:** This defect will be considered for a fix in a release following Fabric OS 4.1.1.
000025799	Medium	**Summary:** Mixed zone does not take effect right after cold reboot. **Symptom:** After enabling a zoning configuration, traffic is running between host on port 58 at domain 10 (10,58) to storage on port 12 at doamin 10 (10,12). These 2 ports are define in a mixed zone: zone: ficon1_lnx17_hba2_zone 10,12 21:00:00:e0:8b:06:67:00 After a cold reboot is done by typing "reboot" on both CPs at the same time and the CPs are in sync again, the traffic does not go through from host (10,58) to storage (10,12). Finisar trace indicates that PLOGI from host to storage is not forwarded to storage port. After typing "cfgdisable" and then "cfgenable ficon_b_all_cascade", the traffic will run through without any problem. **Comment:** The fix for this defect is currently under test.
000025822	Medium	**Summary:** ficonshow ILIR response needs to be cleaned up. **Symptom:** The response to the CLI command 'ficonshow ILIR' contains incomplete information on the LISTENER who received the Implicit Link Incident RLIR frame. The LISTENER information should be removed from this command. **Comment:** The fix for this defect is currently under test.

Defects Closed Since v4.0.2a

The following table lists closed defects since the v4.0.2a release.

Table 3 Defects Closed Since 4.0.2a Release

Defect ID	Severity	Summary
000018525	Critical	Slotpoweroff/Slotpoweron causes slot to lose D_ID . Code has been changed and Slotpoweroff/Slotpoweron does not cause slot to lose D_ID.
000018967	Critical	nsdb_gepn function, which is invoked through API and MS, when writing to freed memory causes corruption. A new variable has been added to hold response CT instead of wrongly using the request CT.
000019034	Critical	FLOGI storm causes the switch to failover due to rejecting the FLOGI on a loopback. The code has been changed to accept the FLOGI, rather than rejecting it to prevent the switch from failing over.
000017838	Critical	Inability to ping or telnet to switch. Data is still running but switches cannot be managed. The interrupt mitigation code was changed to use the "Smart Reset" feature of the ethernet hardware rather than disabling the MAL temporarily.
000022631	High	If a cable is continuously pulled from one L port with a device using ALPA 0xEF, the other L port in the same quad will occasionally start to LIP. The timeout frame on list0 is not removed, which prevents the timeout flag from being cleared.
000023119	High	After a host reboot the switch port is faulted before the HBA can establish a connection with the switch port. This problem is only observed with QLogic 2310 with BIOS 1.30 not with any other versions of the Qlogic HBA or BIOS. This issue is resolved with 4.0.2d and QLogic BIOS v1.34.
000024156	High	Semaphore blocking occurs when a Terminal server flow control is set to on. Flow control enabled on a terminal server connected to the serial port of a switch can cause the switch to hang and telnet and serial ports to become inaccessible. The following commands shellFlowControlEnable and shellFlowControlDisable were added to address this issue. shellFlowControlDisable is the default setting.
000024574	High	L-Port cannot be re-initialized after the HDS RCU's hot code load.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000024217	High	**Summary:** Switch not sending enough LIPs to transition from AL-PA sequence to Old_Port. **Solution:** Defect was closed by documentation of work-around
000024312	High	**Summary:** 'RTC_RD_TIME: Invalid Argument' error message on Standby CP during firmwareDownload procedure. **Symptom:** The Standby CP reported an invalid argument error during a firmwareDownload.
000024854	High	**Summary:** Executing switchdisable/enable and saw ASSERT - Failed expression: NULL. **Symptom:** After running stress tests for several days on a large fabric, as the next set of stress tests were being prepared, an ASSERT was seen indicating that a kernel operation failed when the switch was enabled.
000025162	High	**Summary:** 3900 Panic on v4.1Beta 2 after upgrade from v4.0.2c. **Symptom:** When upgrading from v4.0.2c to v4.1_beta2, a panic was observed on a SW3900. **Solution:** Defect closed as non-reproducible with customer consent.
000025531	High	**Summary:** Running a stress test script over night caused software watchdog to reboot the Standby CP on a core switch. KSWD, uSWD critical errors, also secd and panic core files were created. **Symptom:** Running a stress test script where switches in the secure fabric continuously run: switchdisable/enable, switch speed set to 1G/2G/AN, disable/enable trunking, secfcsfailover, create/activate and remove/activate a security policy commands, with core-edge type topology, could cause a standby CP to reboot.

Table 3 **Defects Closed Since 4.0.2a Release (continued)**

000025606	High	**Summary:** psd dies when switchdisable/switchenable script running in very large fabric. **Symptom:** With 2+4+28 mixed configuration, which has 6 12000s, 6 3800s, 22 3900s, ~700 device ports, 95Kbytes zone size, and traffic. **Action:** running a switchdisable/switchenable script on all 4.1 edge switches (include 4 12000s and 22 3900s) at the same time. The script is: 1. Send command "switchdisable" to all 26 switches at the same time. 2. Sleep 60s 3. Send command "switchenable" to all 26 switches at the same time. 4. Sleep 600s. 5. Repeat step 1, 2, 3, 4 again. **Results:** psd dies on two 3900s with message "Switch: 0, Critical kSWD-kSWD_GENERIC_ERR_CRITICAL, 1, kSWD: '[12]psd:0'...".
000025669	High	**Summary:** Booting over SAN issues on Brocade 12000, v4.1.0_rc2 firmware. **Symptom:** Boot over SAN fails
000025703	High	**Summary:** After about 9.5 hours of stress test, core switches panicked with "Application zoned from switch Instance 0 failed to refresh" message. **Symptom:** Core switches can panic after a long stress operation that causes the fabric to become unstable.
000025717	High	**Summary:** Need updates applied to FA-MIB as outlined below. **Symptom:** A new trap should be sent from switch when CP/Blade/WWN cards get failure. **Solution:** Monitor CP failure, WWN failure and Blade failure to update switch state. Add policy for these 3 monitors. This has been requested by RFE 2745 Need to send an connUnitStatusChange trap when any of these monitored objects matches the policy.

Table 3 Defects Closed Since 4.0.2q Release (continued)

000025781	High	**Summary:** Message "Critical SYSC-ERROR, 1, sysc_main.c:214", and emd dies when script switchdisable/enable running. **Symptom:** With 2+4+28 mixed configuration, which has 6 12000s, 6 3800s, 22 3900s, ~700 device ports, 95Kbytes zone size, and traffic. **Action:** running a switchdisable/switchenable script on all 4.1 edge switches (include 4 12000s and 22 3900s) at the same time. Results in a SW Watchdog error being detected. **Solution:** This defect was caused by an invalid configuration installed on the test station. This invalid configuration was caused by a corrupted set of data structures generated by an internal FICON code build that was on the switch prior to the upgrade. This defect cannot be recreated when upgrading or downgrading between official versions of 4.1.0 and 4.1.1 code releases.
000025792	High	**Summary:** The Cp should not allow the active cp to failover to a missing or non- redundant cp blade.
000025827	High	**Summary:** get fcpd core dump after running the script overnight: doing login to the switch, switchenable, logout. **Symptom:** Running an overnight script that issues switchenable to the same switch over and over, a panic and core dump was observed. Overnight scripts that issue switchenable, switchdisable, switchenable, over and over are able to run for the entire night.
000025887	High	**Summary:** kSWDs being encountered along with full CF error condition. **Symptom:** Over a long period of time running with an application that attempts to login with the switch but fails due to invalid passwords, the switch will encounter a kSWD panic and reboot. Some switches have also exhibited a full CF along with the kSWD error.
000025891	High	**Summary:** Switch Panic, KSWD Error for MSD Failure Caused Reboot and Core Dump. **Symptom:** CP was marked faulty, due to KSWD error when MS Daemon failed causing the CP to failover and reboot.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025893	High	**Summary:** Switch Panic, KSWD Fabric Watch Daemon Caused A Reboot Of Switch and Core Dump. **Symptom:** CP was marked faulty, due to KSWD error when Fabric Watch Daemon failed, CP was failedover and rebooted.
000025894	High	**Summary:** CF(Compact Flash Memory) Full 100% Capacity; Writes Failures Seen. **Symptom:** Writes to compact flash will fail.
000025906	High	**Summary:** Using API Lib 3.0.0a_0530, with firmware v4.1.1_rc2_bld02, API performance is severely degraded.
000019740	High	The switch reboots due to spurt of Loss of Sync interrupts. The code has been changed to monitor the number of LLI interrupts and if the number goes beyond the threshold, the port will be faulted.
000021225	Medium	**Summary:** After failover SECd died and caused new active CP to rebootSymptom: While performing fail-over testing, the security module failed and caused the system to reboot.
000023384	Medium	**Summary:** Running a switchcfgtrunk script on 2+6 SW 12000 fabric caused msd core dump. **Symptom:** Running a stress test that continuously configured and unconfigured switches to support Trunking in a mixed fabric, a Management Server daemon panic was observed.
000023877	Medium	**Summary:** Call AddAttributes to modify AlarmState and AlarmLevel attributes of FwFruCfg object to invalid values returns SUCCESS. **Symptom:** Call AddAttributes to modify AlarmLevel attributes of FwFruCfg object to invalid values returns SUCCESS. **Solution:** Add function fwValidateFruAlarm to verify fru alarm state and level before setting.
000024553	Medium	**Summary:** Upon running diag, SW 12000 switch core dumps in Management Server daemon. **Symptom:** Running a diagnostic through the Fabric Access API caused the switch to panic and reset.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000024660	Medium	**Summary:** Firmwaredownload with option -sf on standby CP:" Oops: kernel access of bad area, sig: 11; TASK = c301c000[2195] 'rpm' Last syscall: 181 ". **Symptom:** Firmwaredownload on single CP (standby CP) gets error Oops kernel access; system will abort the download process and goes back to original firmware version.
000024695	Medium	**Summary:** In some rare occurrences, zone DB may get out of sync after fabric merge under security. Usually involves large zone DB (128 k). **Symptom:** Test case that exceeds documented boundaries. A zoning DB that is larger then the maximum size supported on 3.1 switches is downloaded to a 4.1 switch in a mixed fabric. The 3.1 switches are appropriately segmented from the 4.1 switches after this happens. Then the security version stamp is reset to zero, and a valid sized zoning DB is downloaded to a 3.1 switch which is a backup FCS switch, which is then enabled so that it will join the fabric. Then a second 3.1 switch is disabled/enabled to cause it re-join the fabric, but in some rare instances, this second 3.1 switch remains in a segmented error state.
000024697	Medium	**Summary:** Add non-FCS switch to FCS policy and activate the policy, the non-FCS version stamp becomes "0" **Symptom:** Add non-fcs switch to fcs_policy and activate the policy. Once activation is done, will see the newly added switches are in "Error" status when do secfabricshow. The version stamp on those switches is "0". Security fabric will not see those newly added backup FCS.
000024794	Medium	**Summary:** FirmwareDownload failed due to out of disk space or timeout. This happened on SW 12000 (by Fabric Manager) & SW 3900 (by CLI) .
000024879	Medium	**Summary:** Switch stays in 'Red' state in Fabric Manager display; Status reason in events says 'Switch is Not Responding'. Eventually the switch could run out of memory.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000024890	Medium	**Summary:** (negative testing) run "systemverification" on both logical switches at the same time. Switch will run out the memory within 5 minutes. **Symptom:** Negative test case: Running "systemverification" on both logical switches on the same time will cause the switch to run out memory. **Solution:** Closed by documentation: Systemverificationtest is specifically designed to operate and diagnose both logical switches simultaneously. This command only needs to be run against one logical switch, and both logical switches will be verified. Running this test on both logical switches at the same time causes a duplication of the verification diagnostic to be run, and an over subscription of free memory.
000024923	Medium	**Summary:** Users should not be allowed to create new Node-WWN zoning configuration, when OPTION_POLICY is activated. A warning message should also be displayed. **Symptom:** If OPTION_POLICY is selected to request that no Node WWN zoning should be allowed, and then later they attempt to create a zone with node WWNs: The zoning transaction is appropriately not allowed to be activated, but the error message as to why the zoning request was not allowed does not clearly state it was due to the OPTION_POLICY enforcement.
000024972	Medium	**Summary:** Call AddAttributes to modify SwitchTime attribute of Switch object when External Clock Server is running returns SUCCESS, should return error.
000024997	Medium	**Summary:** Improper error code is returned (-87 ERR_SWITCH_ALLOCATION_FAILURE) when calling GetObjects() w/ OID for a HBA that has dropped out of the fabric.
000025008	Medium	**Summary:** Error message "PD_TRACE-GENERIC" appearing in log file after rebooting the switch every time. **Symptom:** Will see this message every time the switch is rebooted. Message is very misleading to the customer.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025043	Medium	**Summary:** Continuously ping the SW12000 fcip address from the SW3900, and do hafailover on the SW12000. Then OOPS occurs on the SW3900. **Symptom:** This is a stress test in which a denial of service type attack is performed via the in-band FCIP protocol. A SW12000 was continuously issued pings through a SW3900 switch. When a fail-over of the SW12000 took place, the SW3900 saw a panic and a reboot.
000025134	Medium	**Summary:** Running stress test to perform security policy operations, transaction flag will out of sync.
000025196	Medium	**Summary:** Unable to get Telnet Parity or SwitchSupportLog when the target switch Ethernet cable is disconnected. The GET call returns -1(ERR_INVALID_FABRICLIST) or -56(ERR_ACCESS_ERROR). **Symptom:** The Fabric Access API command requests SwitchFSPFInterface, SwitchMemoryUsage, SwitchStatus, SwitchVoltageLevel and SwitchCoreFiles) GetObjects/GetSingleObject are unable to retrieve their data objects when the target Ethernet cable is disconnected.
000025256	Medium	**Summary:** When RLSServiceEnable attribute of Switch Object is DISABLED, GetObjects on PortErrorsOID of NPort object should return error, still succeeds. **Solution:** Add check for DisabledRLS to interface functions.
000025286	Medium	**Summary:** EV_API_DOWNLOAD_SUCCESS is still received immediately after issuing FWDLSelf. **Symptom:** This is a Fabric Access API issue, in which the Success message for a firmwaredownload is given immediately after issuing the command, even though the download itself may take several more minutes to complete.
000025363	Medium	**Summary:** When Target Switch is a 4.1 Switch (doesn't matter about proxy switch), GetObjects or GetSingleObject on SwitchErrorLog OID Multiple Times, API returns Corrupted Error Log Data ! **Symptom:** The Fabric Access API fails to recognize an error occurring during retrieval of the error log from the switch.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025400	Medium	**Summary:** Restricting API access to local Fabric Manager host causes transaction to be held until failover. **Symptom:** Creating an empty API policy through the FM Security admin screen, and responding YES to the warning about restricting API access, while the API is currently connected to the switch, causes management of the Security features to be locked out.
000025451	Medium	**Summary:** Able to download zoneset using CfgDownload. **Symptom:** The Fabric Access API was able to download a new zoneset when it was expected to have that functionality blocked.
000025469	Medium	**Summary:** 4.1 FabWatch, EncodeFWThresholdEntry using invalid Index, GetSingleObject on the FWOID returns -102(INVALID_CLASS_AREA) instead of -103(INVALID_INDEX) **Solution:** thaThresholdStructGet command was returning 0 on success and -1 for all failure cases. It should have returned an error code that identified the specific error.Modified return value in library call such that it returns the proper failure code rather than always returning -1 on any error. In addition, a bug within *InvalidIndex functions where negative numbers were not evaluated as invalid was fixed.
000025517	Medium	**Summary:** Port LED behavior with segmented trunk ports. **Symptom:** Only the trunk master shows a blinking green light if the switches are segmented. The other trunk member shows a solid green light, which leads one to suspect there is no problem with that link. All trunk members should blink indicating an error condition.
000025529	Medium	**Summary:** cfgenable different cfg files in a loop resulted in rcsd failed to refresh SWD. **Symptom:** Running an overnight script in which different Zoning configurations are enabled over and over in a loop. Configurations switch between hardware-enforced Zoning and soft Zoning, and the configuration is enabled from a different switch in the fabric each time. Running on a 16-switch fabric, a Software Watchdog failure was detected.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025544	Medium	**Summary:** Error message is misleading to the end user. **Symptom:** Error messages are not at user level, and do not reflect actual area of failure.Messages: hilsetfruHistory failed, rc=4 for WWN2, WWN 2 removal, WWN 2insertion, WWN 2 not present. **Solution:** The fix refines the 6 messages related to an intermittent inability to access the WWN FRU, to more clearly indicate what failed and how.
000025562	Medium	**Summary:** Oops: kernel access of bad area, sig: 11 during firmwaredownload. **Symptom:** When doing repeated firmwaredownloads of both 12K and 3900 in parallel over a long period of time might experience a kernel panic with message "Oops: kernel access of bad area, sig: 11"
000025569	Medium	**Summary:** Incorrect failover with > 32 zone groups or > 128 devices on a quad during filter recovery. **Symptom:** The problem can show up in one of two scenarios:Both scenarios require you to have loop devices, this problem will not show up with F-port devices. 1. If you have more then 32 zone groups within one quad (four ports). This means that if you have enough loop devices, and they are all zoned to unique hosts such that more then 32 unique groupings need to be defined within the CAM tables or 2. If you have more then 128 devices total per quad (four ports). If you had a large enough configuration of loop devices in a zoning configuration described above, then a fail-over may improperly zone out the devices that go beyond the limits shown above.
000025573	Medium	**Summary:** sfpShow output is not consistent across 3800, 3900 and 12000.
000025597	Medium	**Summary:** HBAFirmwareDownload fails unexpectedly over short and/or long time periods with error -1000. **Symptom:** While running a stress test that performs continuous HBA firmware downloads to multiple HBAs, sometimes an error -1000 is observed on one or more HBAs.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025612	Medium	**Summary:** Configupload does not accept parameters from command line **Solution:** Parser expected all parameters to be in a single string; combined multiple arguments into single string.
000025647	Medium	**Summary:** some of the 3.1 switches are not receiving HBA related API events. **Symptom:** When a Fabric OS 4.1 switch was used as the proxy switch, some HBA-related API events were not delivered to Fabric OS 3.1 switches.
000025653	Medium	**Summary:** change telnet timeout default to 10 minutes in v3.0.2c, 2.6.0.c.
000025682	Medium	**Summary:** BootP installation of v4.1.0 FOS does not load properly on SW3900 switches. **Symptom:** Overwriting the switch Flash by running the "install" script, does not properly load the v4.1.0 FOS in the primary and secondary partitions.
000025732	Mediuim	**Summary:** Unzoned Name Server (MS) should reject any registrations or deregistration command codes. **Symptom:** Customer will be able to issue Register/Deregister Name Server Command Codes via Management Server Unzoned Name Server sub-type.
000025743	Medium	**Summary:** passwddefault command will be executable in the backup switch.
000025751	Medium	**Summary:** Get a lot of messages "FSSK 2: fcsw1-swc: FSSK 2: too many concurrent TX" when fabric is reconfigured; then out of memory happened. **Solution:** Defect was caused by the temporary presence of a bad fix for another defect that has since been corrected. This symptom caused by this defect will not be seen in any official released version of code.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025756	Medium	**Summary:** switchdisable, wait 5 secs, switchenable, wait 20 sec, and haFailover: then fabric keeps reconfiguring. **Symptom:** the fabric keeps reconfiguring after doing the following stepsswitchdisable, sleep 5 secs, switchenable, sleep 20 sec, hafailoverthe workaround is do switchdisable and switchenable, then the fabric will be stable. **Solution:** Defect was caused by the temporary presence of a bad fix for another defect that has since been corrected. This symptom caused by this defect will not be seen in any official released version of code.
000025763	Medium	**Summary:** When 'ctrl-c' is entered before the login completes, it drops to a shell prompt with no path. **Symptom:** When 'ctrl-c' is entered before the login completes, it drops to a shell prompt with no path available. This is easily reproducible in v4.1.0 and all previous v4.x versions of firmware as root. This does not occur as admin.
000025770	Medium	**Summary:** Switch panic with msd and psd core files. **Symptom:** After upgrading from an internal FICON code release to v4.1.1, a switch panic was seen shortly after the switch started running. **Solution:** This defect was caused by an invalid configuration installed on the test station. This invalid configuration was caused by a corrupted set of data structures generated by an internal FICON code build that was on the switch prior to the upgrade. This defect cannot be recreated when upgrading or downgrading between official versions of 4.1.0 and 4.1.1 code releases.
000025800	Medium	**Summary:** Cannot disable timeout value for logical switch 1 of SW12000 switch. **Symptom:** Disabling telnet session timeout value for logical switch 1 of a 12K switch will not work correctly
000025807	Medium	**Summary:** fail on upgrading firmware to 4.2, cause EM core.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000025809	Medium	**Summary:** In Web Tools event log, enabling a zone config does not register an event. **Symptom:** Enabling a new zone config file does not register an event.
000025828	Medium	**Summary:** Occasionally, some ports are still disabled after bladeEnable, immediately followed by haFailover. **Symptom:** If blades are being enabled in the chassis and haFailover was initiated for some reason, at the same time, some switch port blades are marked disabledSolution: Fixed in the 4.1.2 Fabric OS Reference, see attachment.
000025877	Medium	**Summary:** JBOD disk disappearing after reboot. **Solution:** code changes to vary the old fixed value of LISM. The new LISM timeouts will be from 100 ms to 400 ms.
000025882	Medium	**Summary:** secFabricShow and fabricShow have different number of switches. **Solution:** Closed as not reproducible
000025905	Medium	**Summary:** After the download is completed on standby getting VERIFY - Failed expression: newPdbP != NULL, file = ucast.c, line = 1347, user mode args = 7, 10, 52, 54 **Symptom:** After all package is downloaded successfully on standby CP, in the middle of hafailover, a VERIFY error was reported. However, the download still completed, and the switch still functions normally.
000016535	Medium	The chassis serial number is not stored with unit, remote dispatch of service hampered. Need addition of chassis serial number for unit identification through CLI and GUI. The chassis serial number has been added to the "Info" panel within WebTools switchview and the chassisshow command for CLI.
000017744	Medium	During Random changes from healthy to marginal the warning by the switch in fabric testing at 40 deg C. the switch status message does not include a reason. The code has been changed to add the reason string to switch status message.

Table 3 Defects Closed Since 4.0.2a Release (continued)

000018128	Medium	'rpcd' processes are left in a "zombie" state because an API application connection is broken abnormally. The processes should be cleaned-up within 2 hours, but are continuing to exist indefinitely until the switch is rebooted. The code was changed so that the semaphore is cleared which the cleanup handler was waiting for.
000019518	Medium	E-port Link Timeout from silkworm 2800 switches in a 20 switch mixed fabric.
000017195	High	A message Bloom_Bad_ID is reported during fabric instability. This is only a warning message. The BLOOM-BAD_ID error log level was changed from Critical to Warning.
000017309	Low	BurninStatus command does not issue correctly. A path was added for the Linux commands to allow admin login to run burninststus.
000027717	Low	**Summary:** In Web Tools Event log, clicking on time doesn't sort it by the time and no year included in date. **Symptom:** When events in eventlog span a year boundary, the events may not be listed in the proper order. **Customer Impact:** A fix would be implemented in the next maintenance release following 4.1.1.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

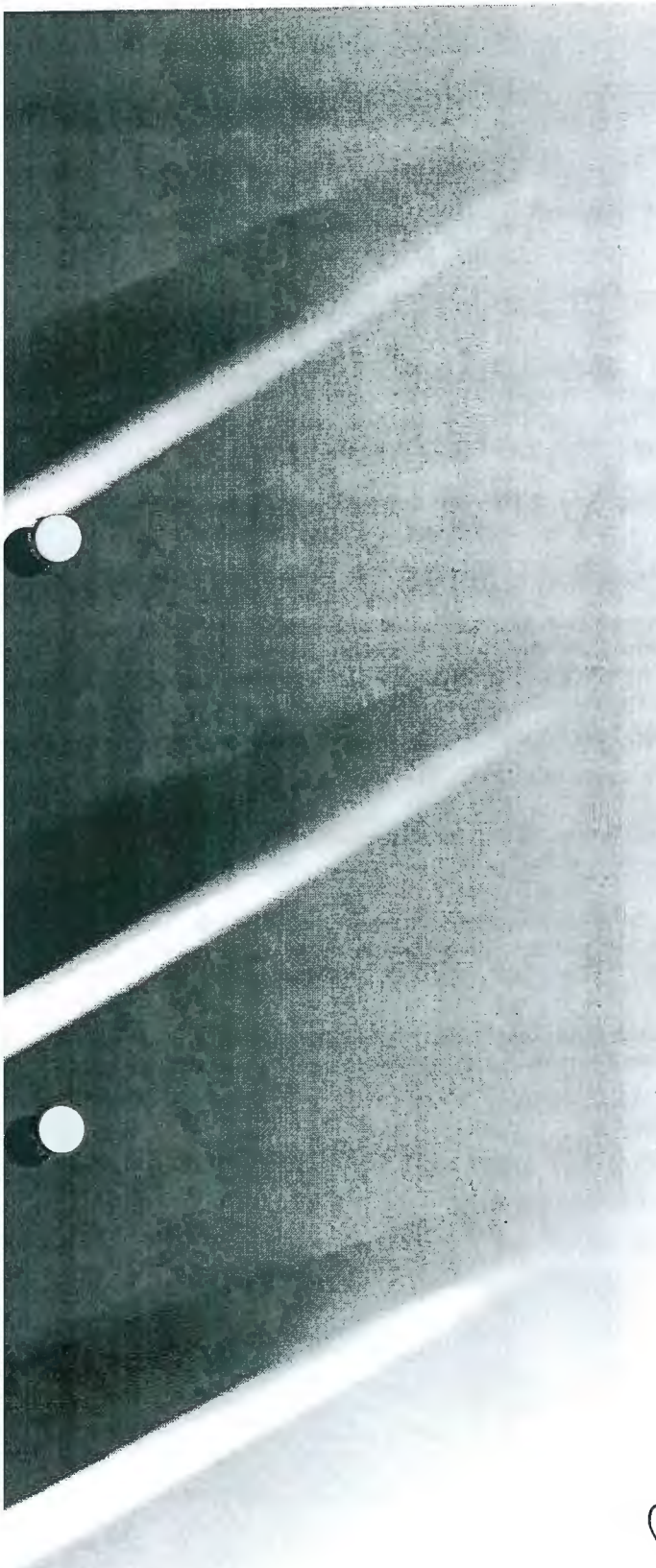
Trademark Information

EMC², EMC, Symmetrix, AutoIS, CLARiiON, CLARalert, DG, E-Infostructure, HighRoad, Navisphere, PowerPath, ResourcePak, SRDF, VisualSAN, WideSky, and The EMC Effect are registered trademarks and EMC Automated Networked Storage, EMC ControlCenter, EMC Developers Program, EMC Enterprise Storage, EMC Enterprise Storage Network, EMCLink, EMC OnCourse, EMC Proven, EMC Snap, Access Logix, ATAtude, AutoAdvice, Automated Resource Manager, AVALONidm, C-Clip, CacheStorm, Celerra, Celerra Replicator, Centera, CentraStar, CLARevent, Connectrix, CopyCross, CopyPoint, CrosStor, Direct Matrix, Direct Matrix Architecture, EDM, E-Lab, Enginuity, FarPoint, FLARE, GeoSpan, InfoMover, MirrorView, OnAlert, OpenScale, PowerVolume, RepliCare, SafeLine, SAN Architect, SAN Copy, SAN Manager, SDMS, SnapSure, SnapView, SnapView/IP, StorageScope, SymmAPI, SymmEnabler, Symmetrix DMX, TimeFinder, Universal Data Tone, and where information lives are trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ANEXO SWITCH TIPO 03
PARTE 8

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel.: 21 2442-8800
www.cobra.com.br



EMC Connectrix B Series Zoning

Version 3.1 and Version 4.1

REFERENCE MANUAL

P/N 300-000-639
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

Connectrix B Series systems have been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Preface

The EMC Connectrix B Series Zoning provides information on zoning that you may encounter during installation and operation of the DS-16B2, DS-32B2 and ED-12000B.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch and Enterprise Director. For the most up-to-date information on product features, see your product release notes.

If a feature in the DS-16B2, DS-32B2, or ED-12000B does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

This manual is part of the EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and ED-1200B documentation set, and is intended for use by administrators of the DS-16B2, DS-32B2, and ED-1200B switch.

Readers of this manual are expected to be familiar with the EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and ED-1200B operating environment.

Organization

Here is an overview of where information is located in this manual.

- Chapter 1, *Introducing Zoning*, provides information on initial configuration zoning procedures.
- Chapter 2, *Using Zoning*, provides information on working with zoning.

- Chapter 3, *Using QuickLoop Zones* explains how zoning can be used to zone QuickLoop.
- Appendix A, *Zoning Concepts and Guidelines*, provides information on Zoning concepts and guidelines.
- Appendix B, *Zoning and Secure Fabric OS*, explains how to use zoning to administer security.
- Appendix C, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix Departmental Switch DS-16B2 .
- The *Glossary* defines terminology used in this manual.

Related Documentation

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*

- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used In This Manual

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this manual:

Palatino, bold	• Dialog box, button, icon, and menu items in procedures • Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	• New terms or unique word usage in text • Command line arguments when used in text • Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	User entry. For example: **`symmpoll -p`**
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.EMC.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.EMC.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to `techpub_comments@EMC.com` with your opinions of this manual.

1 Introducing Zoning

This chapter explains how Zoning can be used for:

Overview

Zoning allows you to partition your Enterprise Storage Network (ESN) into logical groupings of devices that can access each other. Every zone has at least one member. Empty zones are not allowed. Using zoning, you can arrange fabric-connected devices into logical groups, or zones, over the physical configuration of the fabric.

Zones can be configured dynamically. They can vary in size depending on the number of fabric-connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

Administering Security

Use zones to provide controlled access to fabric segments and to establish barriers between operating environments. For example, isolate systems with different uses or protect systems in a heterogeneous environment.

Customizing Environments

Use zones to create logical subsets of the fabric to accommodate closed user groups or to create functional areas within the fabric. For example, include selected devices within a zone for the exclusive use of zone members, or create separate test or maintenance areas within the fabric.

Optimizing IT Resources

Use zones to consolidate equipment, logically, for IT efficiency, or to facilitate time-sensitive functions. For example, create a temporary zone to back up nonmember devices.

Figure 1-1 illustrates three zones with some overlap. It also contains devices that are not assigned to a zone, and are thus not active in the fabric if zoning is enabled.

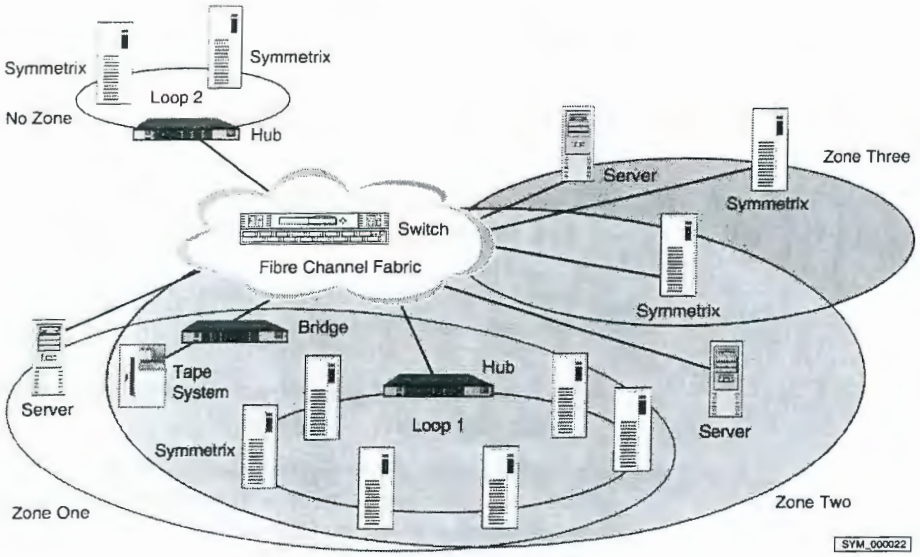


Figure 1-1 Fabric With Three Zones

Implementing Zoning

Implementing zoning simplifies the zoning process in the following ways:

- You can administer zoning from any switch in the fabric. Configuration changes made to one switch are automatically replicated to all switches in the fabric; if a new switch is added to an existing fabric, all zone characteristics are automatically applied to the new switch. Because each switch stores zoning information, zoning ensures a high level of reliability and redundancy.

- Zones can be configured dynamically. When configuring new zones:
  - Data traffic on ports and devices is idle for a moment, and then resumes according to the new zoning configuration.

    Some hosts might need to be rebooted to ensure you are not accessing previously zoned devices.

  - Data traffic across interswitch links (ISLs) in cascaded switch configurations is not affected.
- Zoning uses policy-based administration. Because zoning uses policy based administration — separating zone specification from zone enforcement — you can manage multiple zone configurations and easily enable a specific configuration when it is required. A fabric can store any number of zone configurations; however, only one configuration is active at a time. Because the configurations are predetermined and stored, a new configuration can be easily enabled.
- Zoning can be configured and administered with either Telnet commands or Web Tools.

  For information on Telnet commands, refer to the *DS-16B2 Fabric OS Reference Manual* or the *DS-32B2 and ED-12000B Fabric OS Reference Manual*. For information on Web Tools, refer to the *DS-16B2 Web Tools User Guide* or the *DS-32B2 and ED-12000B Web Tools*.

License Activation

Licenses can be activated using two methods; Telnet or Web Tools. Use the following procedure to determine if a specific license is activated. Use the *licenseShow* command to view a list of all licenses activated on your switch, as shown in the example below. If the necessary license is not included in the list, activate the license using either Telnet or Web Tool.

To do this:

1. Log onto the switch by telnet using an account that has administrative privileges.
2. Enter the `licenseshow` command on the telnet command line. A list of all activated licenses on the switch will be generated as shown in the example.

Example

```
switch:admin> licenseshow

SdcReRcbSbjedSfa:
    Web license
SdcReRcbSbjedSfb:
    Zoning license
SdcReRcbSbjedSd:
    QuickLoop license
SdcReRcbSbjedSfe:
    Fabric license
SdcReRcbSbjedSff:
    Remote Switch license
SdcReRcbSbjedSfg:
    Remote Fabric license
SdcReRcbSbjedSfh:
    Extended Fabric license
SdcReRcbSbjedSfj:
    Entry Fabric license
SdcReRcbSbVedSfM:
    Fabric Watch license
SdcReRcbSbXedSfO:
    Performance Monitor license
SdcReRcbSbbedSfS:
    Trunking license
SdcReRcbSbjedSfy:
    Security license
switch:admin>
```

License Activation Using Telnet

To do this:

1. Enter the following on the command line, where the word "key" is the license key provided to you, surrounded by double quotes. The license key is case sensitive and must be entered exactly as given.

   licenseadd *"key"*

2. Verify the license was added by entering the licenseshow command, as shown in the example above. The feature is now activated and available.

License Activation Using Web Tools

If a Web Tools license is activated, Web Tools can be used to activate additional licenses.

To do this:

1. Launch a web browser, enter the switch name or IP address in the **Location/Address** section of the browser, and press **Enter**. Web Tools launches, displaying the Fabric View.
2. Click the **Admin** button on the relevant switch panel. The logon window is displayed.
3. Enter a logon name and password with administrative privileges and press **Enter**. The Administration View is displayed. Select the **License Admin** tab.
4. Enter the license key in the **License Key** field and click **Add**. The feature is now activated.

2

Using Zoning

This chapter explains the concept of zoning and how to use zoning to partition a fabric into logical groupings of devices. Information on using zoning is included in the following sections:

Understanding Zoning

A zone is a group of fabric-connected devices arranged into a specified grouping. Any device connected to a fabric can be included in one or more zones. Devices within a zone possess an awareness of other devices within the same zone; they are not aware of devices outside of their zone.

Zone members (ports, WWNs, or aliases) are grouped into a zone; in turn, zones are grouped in a zone configuration (a collection of zones). Zones can overlap; that is, a device can belong to more than one zone. A fabric can consist of multiple zones.

A zone configuration can include both hard and soft zones (described later) and there can be any number of zone configurations resident on a switch; however only one configuration can be active, that is enabled, at a time. The number of zones allowable is limited only by memory usage.

After zoning has been enabled, if a device is not explicitly defined in a zone, that device will exist in a zone all by itself. The device will be isolated and will be inaccessible by other devices in the fabric.

Figure 2-1 illustrates three zones with some overlap. It also contains devices that are not assigned to a zone, and are thus not active in the fabric if Zoning is enabled.

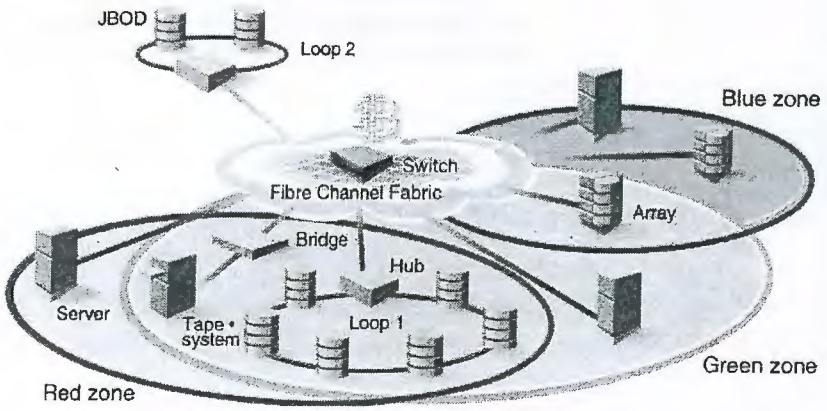


Figure 2-1 Fabric With three Zones

Preparing to Set Up Zoning

Use the following to set up zoning in the Connectrix fabric:

- Create a detailed diagram of the fabric, showing all the switches with their ISLs. The diagram will help to account for every port in the fabric.
- Create an expanded diagram of each switch in the fabric. This diagram will account for every port type in on each switch in the fabric (F_Port, FL_Port, E_Port etc.).
- If the fabric is going to contain private loop devices (QuickLoop), then the user will need to account for this. Refer to *Rules of Zoning Architecture* on page 2-36.
- Consider turning off unused ports, ports that have nothing connected to them, within zoned fabrics. This action will affect the security of the fabric. If Secure Fabric OS is used, a policy to "lock down" ports can be implemented.
- For fabrics with multiple zones enabled, it is generally best to configure one zone at a time and then test it with the Zone Analyzer available in Web Tools. If you create all the zones without testing each zone as it is created, it is difficult to debug. After the first zone is setup in the fabric, the user may plug in devices and then test the connections to confirm that everything is functioning properly.

Zone Definitions

A zone in a fabric is a set of devices that have access to one another. All devices connected to a fabric may be configured into one or more zones. Every zone has at least one zone object. Empty zones are not allowed. The zone objects are described by a separated semi-colon list of member definitions.

The memory constraints for zoning are far larger than the number of devices that can be connected to a fabric. The zone size for EMC Connectrix Fabric OS v4.1.0 is 127726 Bytes. The zone size for Connectrix Fabric OS v3.x and v2.x is 98232 Bytes.

Zone definitions and configurations are consistent across reboots and power cycles. If two switches are connected in a fabric, they can become isolated (for example, due to an ISL failure). When rejoined, they will maintain the same fabric configuration unless one of the switches has had a configuration change.

Zone Objects

A zone object is any other device in a zone and may be any of the following:

- Physical port number (area number) on the switch
- Node World Wide Name
- Port World Wide Name

Objects that are either part of a fabric zone or a QuickLoop zone can be categorized as devices. An object cannot be part of both categories. When zone objects are defined, they are put into zones. One or more zones is a zone configuration.

Zone objects identified by "port number" or the "area number" are specified as a pair of decimal numbers "d,area", where "d" is the Domain ID of the switch and "area" is the area number on that switch, see Table 2-1 on page 2-6.

For example v3.1, "3,13" specifies port 13 on switch number 3. Another example for v4.1.0, "3,46" specifies port 14 on slot number 3 or area 46. When the physical port number specifies a zone object, then all devices connected to that port are in the zone. If this physical port is an arbitrated loop, then all devices on the loop are part of the zone.

Worldwide names are specified as an eight digit hexadecimal number separated by colons, for example "10:00:00:90:69:00:00:8a". When

node name specifies a zone object, all ports on that device are in the zone. When port name specifies a zone object, only that single port is in the zone.

The types of zone objects used to define a zone may be mixed and matched. For example, a zone defined with the following zone objects: "2,12; 2,14; 10:00:00:80:33:3f:aa: 11" would contain whatever devices are connected to switch 2 ports 12 and 14, and a device with the WWN (either node name or port name) "10:00:00:80:33:3f:aa:11" that is connected on the fabric.

Zone Aliases

Zone aliases simplify repetitive entry of "zone objects" such as port numbers or WWN. For example, the name "Eng" could be used as an alias for "10:00:00:80:33:3f:aa:11".

An alias is a name assigned to a device or group of devices. By creating an alias you can assign a familiar name to a device, or you can group multiple devices into a single name. This can simplify cumbersome entries and it allows an intuitive naming structure such as using NT_Hosts to define all NT hosts in the fabric.

Selecting Ports on the ED-12000B

The commands used to administer the Fabric OS v4.1.0 require specific slot and area numbers. These commands use a common specification method. Area numbers distinguish ED-12000B ports that have the same port number but are on different slots. When you specify a particular slot and port for a command, the slot number operand must be followed by a slash (/), followed by the port number value.

In version 4.1.0, since the DS-32B2 does not implement slots, this portion of the operand is not required.

For example, to enable port 4 on a switch blade in slot 2, specify the following:

```
portEnable 2/4
```

The ED-12000B switch has a total of 10 slots. Slot numbers 5 and 6 are control processor cards, and slots 1 through 4, and 7 through 10 are switch cards. Each switch card contains 16 ports counted from the bottom 0 to 15. A particular port is represented by both slot number (1 through 10) and port number (0 through 15).

Zoning commands for Fabric OS v4.1.0 require specifying a port using an area number method, where each port on a particular domain is given a unique area number. Table 2-1 shows area and port mapping for slots 1 through 10 on a switch.

Table 2-1 **Area and Port Mappings**

Slot Number	Area and Port Mappings on the Switch
Slot 1	Area numbers range from 0 to 15 Port numbers range from 0 to 15
Slot 2	Area numbers range from 16 to 31 Port numbers range from 0 to 15
Slot 3	Area numbers range from 32 to 47 Port numbers range from 0 to 15
Slot 4	Area numbers range from 48 to 63 Port numbers range from 0 to 15
Slots 5 and 6	Control Processor Cards
Slot 7	Area numbers range from 0 to 15 Port numbers range from 0 to 15
Slot 8	Area numbers range from 16 to 31 Port numbers range from 0 to 15
Slot 9	Area numbers range from 32 to 47 Port numbers range from 0 to 15
Slot 10	Area numbers range from 48 to 63 Port numbers range from 0 to 15

Zoning Configurations

When zoning is disabled, devices can communicate without regard to zone restrictions. When zoning is enabled, zoning is enforced throughout the fabric and devices can communicate only within their zones.

A switch can maintain any number of zone configurations; however, only up to one zone configuration can be enabled, or enforced, at a time. Because multiple configurations reside in the switch, you can switch from one configuration to another as events dictate. For example, you can write a script to set up a prespecified zone configuration to be enabled at certain times of the day; or, in the event

of a disaster, you can quickly enable a defined configuration to implement your disaster policy.

Zone configurations can be:

- Defined
- Effective
- Saved

Defined

This is the complete set of all zone objects that have been defined in the fabric. When zone objects are defined, the information initially resides in RAM. It must be saved to ensure that it is saved to flash memory and is not lost during:

- New zone configuration
- Power down
- Reboot
- Fastboot
- Power cycles
- CP Failover (for the ED-12000B only)

Effective

This is the zone configuration that is enabled (active). It resides in RAM. It must be saved to ensure that it is not lost during power down. Any changes replicate to all switches in the fabric when the configuration is enabled or saved.

Saved

This is the zone configuration that was last saved. It resides in flash memory and it is persistent. A copy of the "defined configuration" plus the name of the "effective configuration" which is saved in flash memory by the `cfgSave` command. There may be differences between the "saved configuration" and the "defined configuration" if the system administrator has modified any of the zone definitions and has not saved the configuration.

In Figure 2-2, the defined and effective configurations are saved to flash.

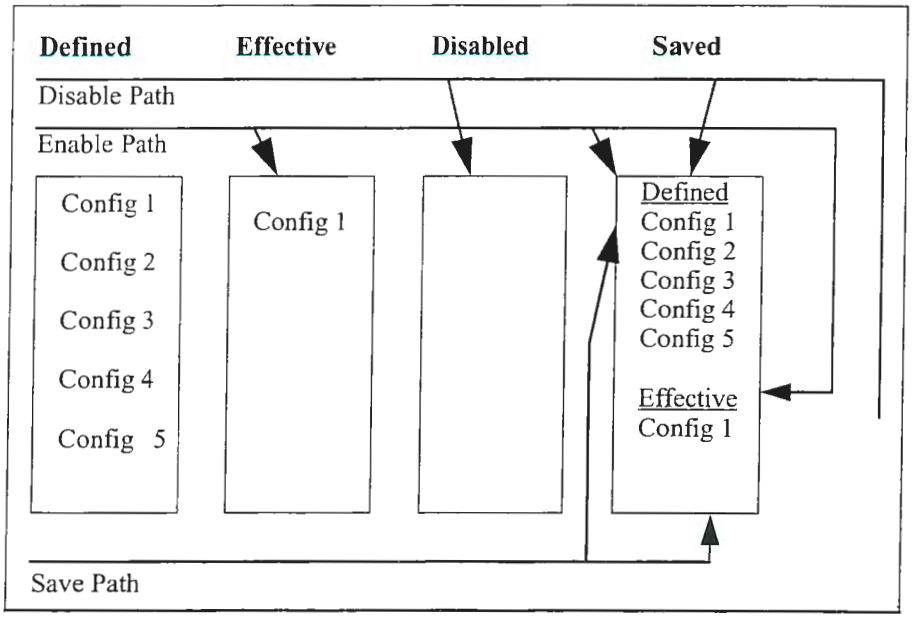


Figure 2-2 Zone Configuration

In Figure 2-3 on page 2-9, Config 5 is defined (created). When it is defined, it resides only in RAM. To permanently store the new configuration and make it accessible across reboots, it must be saved to flash memory.

This can be accomplished by:

- Saving it directly to flash (the recommended method). This saves the defined and effective configurations to flash. If there is no effective configuration, saving it will not enable a configuration.
- Enabling it. This saves the defined and effective configurations to flash.

  In Figure 2-3, zone configurations are defined, enabled, and saved to flash.

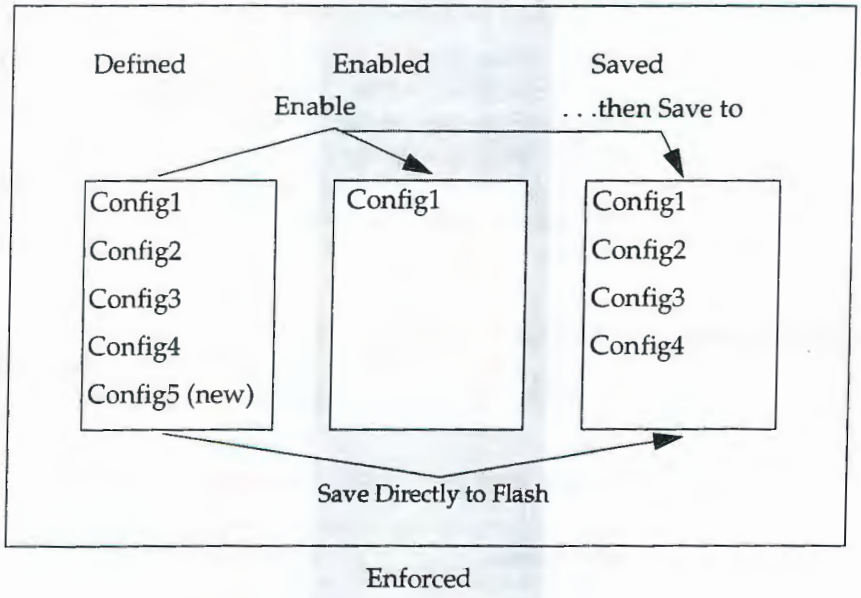


Figure 2-3 Saving a Zone Configuration

- Disabling it. This deletes the effective configuration and saves the defined configuration to flash. There is no effective configuration in the flash at this point.

On power up, the switch automatically reloads the "saved configuration", and if a configuration was in effect when it was saved, the same configuration will be reinstated with an auto run of the `cfgEnable` command.

Only the enabled configuration (in the shaded area) is enforced.

Zoning Management

Zoning may be managed by three methods:

- Logging into the switch via telnet
- Web Tools
- Fabric Manager

Any switch in the fabric can be used to make changes to the zoning configuration. The changes will be replicated to all the other switches in the fabric only if commands that "close a transaction" are used.

When a transaction is opened, all new zoning information is placed in a transactional buffer. The new changes are not applied to the fabric until the transaction is closed. A transaction is aborted when another switch closes its transaction or by issuing the command `cfgTransAbort`. When a transaction is closed, all new and existing zoning information is applied to the fabric and saved to flash memory.

Transactional Model

Zoning commands are executed under the transactional model. A working copy of defined configurations is created at the start of a transaction. Each zoning command is executed from the working copy.

The following commands are issued to open a transaction:

Command	Description
`aliAdd`	Add a member to a zone alias
`aliCreate`	Create a zone alias
`aliDelete`	Delete a zone alias
`aliRemove`	Remove a member from a zone alias
`cfgAdd`	Add a member to a configuration
`cfgClear`	Clear all zone configurations
`cfgCreate`	Create a zone configuration
`cfgDelete`	Delete a zone configuration

`cfgRemove`	Remove a member from a configuration
`cfgTransAbort`	Abort zone configuration transaction (does not update RAM or flash)
`fazoneAdd`	Add a member to a fabric assist zone
`fazoneCreate`	Create a fabric assist zone
`fazoneDelete`	Delete a fabric assist zone
`fazoneRemove`	Remove a member from a fabric assist zone
`qloopAdd`	Add a member to a qloop
`qloopCreate`	Create a qloop
`qloopDelete`	Delete a qloop
`qloopRemove`	Remove a qloop
`zoneAdd`	Add a member to a zone
`zoneCreate`	Create a zone
`zoneDelete`	Delete a zone
`zoneRemove`	Remove a member from a zone

QuickLoop is only supported for version 3.1.

When a transaction is opened, all new zoning information is placed in a transactional buffer. Unless the transaction is closed, the new changes are not applied to the fabric. A transaction is aborted by the `cfgTransAbort`, or when another switch closes its transaction.

Fabric Assist zoning and QuickLoop zoning are not supported by EMC. Therefore, the `fazone` and `qloop` commands are not supported.

To abort a transaction, type the following: **`cfgTransAbort`**.

The following commands are issued to end a transaction:

Command	Description
`cfgDisable`	Disable a zone configuration
`cfgEnable`	Enable a zone configuration
`cfgSave`	Save zone configurations in flash

When a transaction is closed, all new (from the transactional buffer) and existing zoning information is saved to memory (flash) and applied to the fabric.

The following commands do not impact a transaction and are for information only:

Command	Description
`aliShow`	Print aliases
`cfgShow`	Print configuration information
`zoneShow`	Print zone configuration information
`qloopShow`	Print qloop configuration

Zoning Schemes

Zoning schemes are created to isolate systems that have different operating environments. For example, you can create a zone to contain only World Wide Name (WWN) devices. Zoning schemes are created to enforce access of information exclusively to devices in the defined zoning scheme.

The following zoning schemes are available:

Table 2-2 **Zoning Schemes**

Zoning Schemes	Description
Switch/Port Level Zoning	A zone containing members specified by switch ports (domain ID, port number), or aliases of switch ports, only. Port zoning is hardware enforced in the DS-16B, DS-16B2, DS-8B, DS-32B2, and ED-12000 series of switches and beyond.
WWN Zoning	A zone containing members specified by device World Wide Name (WWN), or aliases of WWNs, only. WWN zones are hardware enforced in the DS-16B2, DS-32B2, and ED-12000 switch. WWW zones are software enforced in the DS-16B and DS-8B series or earlier.
AL_PA Level	Members of a QuickLoop are specified by the AL_PA when zoned. Identification other then AL_PA in a QuickLoop cannot be used.
Mixed Zoning	A zone containing some members specified by WWN and some members specified by switch port. Mixed zones are software enforced through the fabric name server only.

QuickLoop is only supported in version 3.1.

Zones can be a hard (hardware enforced), soft (advisory), or broadcast zone. In a hardware enforced zone, zone members can be specified by port number, or by WWN, but not both. A software enforced zone is created when a port member and WWN member are in the same zone.

Zone Enforcement

A zone containing members specified by World Wide Name (WWN), or aliases of WWNs only, are considered WWN zones. WWN zones are hardware enforced in the DS-16B2, DS-32B2, and ED-12000B switches.

A zone containing devices specified by port number or aliases of port numbers only, are hardware enforced zones.

WWN zones are software enforced in the DS-16B and DS-8B switches.

A zone containing one WWN and one port number or aliases of either is considered a software enforced zone.

Zoning service is available on 2 Gb/s platforms, featuring our third-generation ASIC, and adds the ability to perform hardware-enforced zoning for zones defined by WWN, above and beyond hardware-enforced zoning for zones defined by [domain,port] already available on 1 Gb/s platforms.

Zones are either hardware enforced or software enforced depending on the scheme that is used. When a zone is specified by either port number (area number) or WWN, but not both it will be a hardware enforced zone.

The difference between hard and soft zoning is that hard zoning is enforced at the Name Server level, as well as the Application-Specific Integrated Circuit (ASIC). Soft zoning is exclusively enforced through selective information presented to end nodes through the fabric simple name server (SNS). With hard zoning, each ASIC maintains a list of source port IDs that have permission to access any of the ports on that ASIC. The ASIC hardware blocks inappropriate frames from passing through it, dropping them if they attempt to talk outside their zones.

Hardware Enforced Zones

In a hardware enforced zone, all zone members are specified as either switch ports or WWN, but not both. Any number of ports or WWNs in the fabric can be configured to the zone. When a zone member is specified by port number or WWN, the individual device port or WWN is included in the zone.

Hardware-enforced zoning means that each frame is checked by hardware before it is delivered to a zone member and discarded if there is a zone mismatch. This can be defined in two ways for 2 Gb/s switches:

- All zone members in a given zone are defined by WWNs
- All zone members in a given zone are defined by [domain,port]

If WWNs are used exclusively in a zone, new devices can be attached without regard to physical location. In hard zones, switch hardware ensures that there is no data transferred between unauthorized zone

members. However, devices can transfer data between ports within the same zone. Consequently, hard zoning provides the highest level of security.

Software Enforced Zones

In a software enforced zone, at least one zone member is specified by WWN and one member is specified as a port. In this way, you have a mixed zone that is software enforced. When a device logs in, it queries the name server for devices within the fabric. If zoning is in effect, only the devices in the same zone(s) are returned. Other devices are hidden from the name server query reply.

Zoning software limits access to data by segmenting a fabric into virtual private ESNs. Available on both 1 Gb/s and 2 Gb/s platforms, software-enforced zoning prevents hosts from discovering unauthorized target devices, while hardware enforced zoning prevents a host form ever accessing a device it is not authorized to access.

Software enforced zones are created when a combination of WWNs and ports are used. When using software enforced zones, the switch does not control data transfer and there is no guarantee of data being transferred from unauthorized zone members. Use software zoning where flexibility and security are ensured by the cooperating hosts.

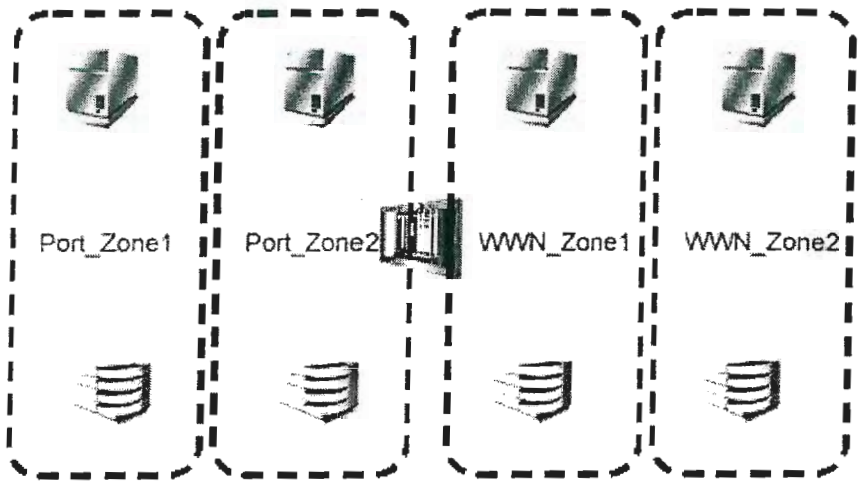


Figure 2-4 Hardware Enforced Zoning (no port and WWN overlap)

Overlapping zones (zone members appearing in multiple zones) are permitted and hardware enforcement will continue as long as the overlapping zones have either all WWNs or [domain,port] entries.

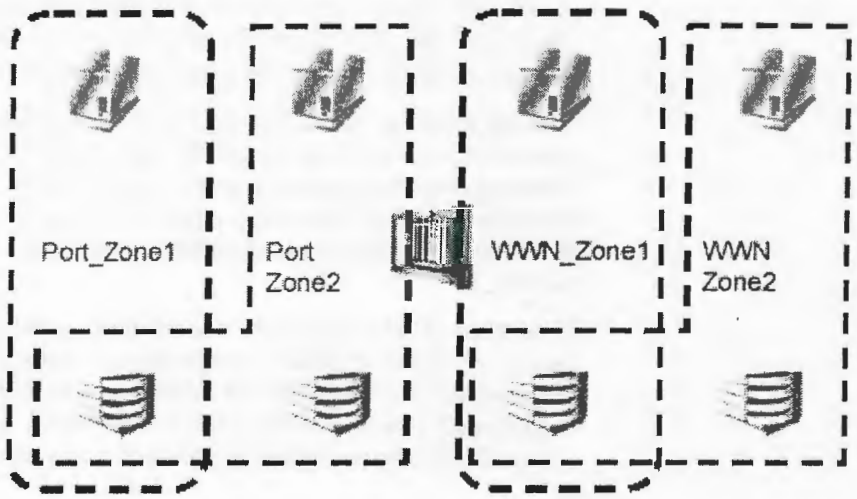


Figure 2-5 Overlapping Hardware Enforced Zoning

Any zone comprised of WWNs and [domain,port] entries on the 2 Gb/s platform rely on Name Server authentication as well as hardware (ASCI) assisted authentication, which ensures that any PLOGI/ADISC/PDISC/ACC from an unauthorized device attempting access to a device it is not zoned with would be rejected. 2 Gb/s switches always deploy the hardware assist in any zone configuration.

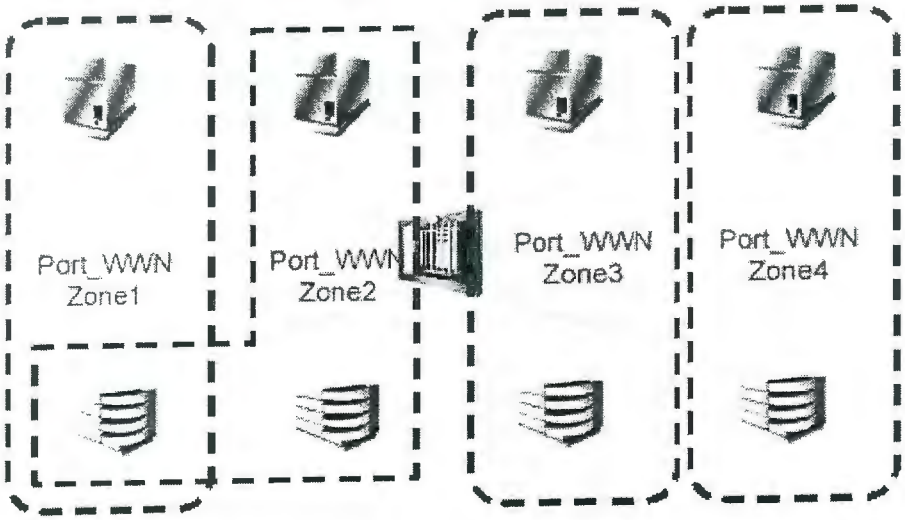


Figure 2-6 Zoning With Hardware Assist (mixed port & WWN zones)

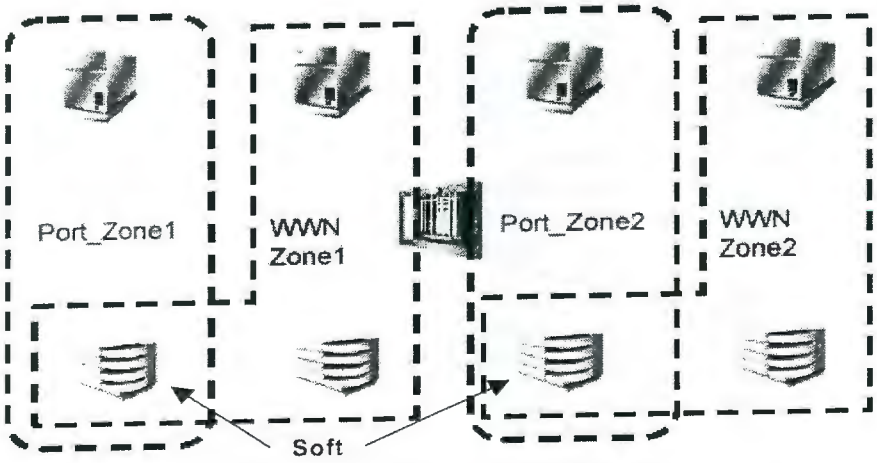


Figure 2-7 Overlapping Hardware Enforced Zoning With Soft Porting (i.e., only the ports that are overlapped will be Software enforced with Hardware Assist)

When zoning is disabled, the fabric is in a non-zoning mode and devices can freely access other devices in the fabric. When zoning is enabled, zoning is enforced throughout the fabric and devices can communicate only within their zones

To discern if a zone is hardware-enforced, use either the **portzoneshow** or **portcamshow** command, as shown in the following example:

Example

```
ulys11_sw1:root> portzoneshow

PORT: 16   Enforcement: E-PortdefaultHard: 0F-port: 0
PORT: 17   Enforcement: E-PortdefaultHard: 0F-port: 0
PORT: 18   Not Zoned
   PORT: 19   Not Zoned
   PORT: 20   Not Zoned
   PORT: 21   Not Zoned
   PORT: 22   Not Zoned
   PORT: 23   Not Zoned
PORT: 24   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 25   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 26   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 27   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 28   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 29   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 30   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 31   Enforcement: E-PortdefaultHard: 0F-port: 0
   PORT: 32   Not Zoned
   PORT: 33   Not Zoned
   PORT: 34   Not Zoned
   PORT: 35   Not Zoned
   PORT: 36   Not Zoned
   PORT: 37   Not Zoned
   PORT: 38   Not Zoned
   PORT: 39   Not Zoned
   PORT: 40   Not Zoned
   PORT: 41   Not Zoned
   PORT: 42   Not Zoned
   PORT: 43   Not Zoned
   PORT: 44   Not Zoned
   PORT: 45   Not Zoned
   PORT: 46   Not Zoned
   PORT: 47   Not Zoned
   PORT: 48   Enforcement: HARD WWNdefaultHard: 0F-port: 1
   PORT: 49   Enforcement: HARD WWNdefaultHard: 0F-port: 1
   PORT: 50   Not Zoned
   PORT: 51   Not Zoned
   PORT: 52   Enforcement: HARD WWNdefaultHard: 0F-port: 1
   PORT: 53   Not Zoned
   PORT: 54   Not Zoned
```

```
    PORT: 55    Not Zoned
    PORT: 56    Not Zoned
    PORT: 57    Not Zoned
    PORT: 58    Not Zoned
    PORT: 59    Enforcement: HARD PORTdefaultHard: 0F-port: 1
    PORT: 60    Not Zoned
    PORT: 61    Enforcement: HARD WWNdefaultHard: 0F-port: 1
    PORT: 62    Enforcement: SOFTdefaultHard: 0F-port: 1
    PORT: 63    Enforcement: HARD WWNdefaultHard: 0F-port: 1

ulys11_sw1:root>
```

Creating and Administrating Zoning

Zoning can be implemented and administered from any switch in the fabric that has a Zoning license enabled. When a change in the configuration is saved, enabled, or disabled per the transactional model, it is automatically distributed to all switches in the fabric.

Create and Enable a Basic Zone Configuration

To create and enable a basic zone configuration follow the procedure below:

1. Create a zone: `zonecreate "zonename", "ports"`
   - zonecreate "zone_1", "1,0;1,2"
2. Create a zone configuration: `cfgcreate "cfgname", "zonename"`
   - cfgcreate "zonecfg_1", "zone_1"
3. Enable the zone configuration: `cfgenable "cfgname"`
   - cfgenable "zonecfg_1"

Detailed Zone Configuration Procedures

To implement Zoning, follow the procedures below:

1. Review current configurations.
2. Create an alias.
3. Define the zone.
4. Define the zone configuration.
5. Analyze the zone configuration.
6. Enable the zone configuration.
7. Review the enabled configuration.

Each zone object defined — alias, zone, zone configuration — must have a unique name; that is, an alias cannot have the same name as another alias, zone, or a zone configuration.

Naming Convention

Typically, three types of devices can have an alias. These are: the server HBA, the disk storage device, and the tape device. New devices such as virtualization devices may also require an alias. Any device that acts as either a SCSI initiator or SCSI target will have an alias. A suggested scheme follows.

Each alias has three components: device type, device identifier, and port location.

The device type is:

- SRV - for servers
- STO - for storage
- TPE - for tape
- VRA - for virtualization appliance

The device identifier can be the host name for the server, the serial number, or frame identifier for the storage. The port location should allow the administrator to physically find the device port where the fiber is attached. A suggestion would be the PCI slot on a server, the fiber port on the storage frame, or the port on a tape drive. If a unit only has one port, this field can be omitted or identifier "SNG" for single attach used. Some examples:

- SRV_MAILSERVER_SLT5 a server, host name mailserver, in PCI slot 5
- TPA_LTO9_SNG a tape, LTO drive number 9, and it is single attached
- STO_DSK3456_5Ca storage unit, serial id 3456 on the fifth card in port C

The shorter names are easier to remember and are less prone to typing errors. But do not sacrifice meaning for shortness.

In a similar manner, zones should be named for the initiator they contain. For the server alias listed in the Naming Convention section above, the zone would be ZNE_MAILSERVER_SLT5. This clearly identifies the server HBA that is associated with the zone.

Configuration naming is more flexible. In general though, one configuration should be named "PROD fabricname". Fabricname is the name that the fabric has been designated. The purpose of the PROD configuration is to easily identify the configuration that can be implemented and provide the most generic services. If other configurations are used for specialized purposes, the names such as: "BACKUP_A", "RECOVERY_2", "TEST_18jun02" may be used.

Review Current Configurations

Use the `cfgshow` command to show all currently defined configurations and the effective configuration.

```
test180_Jr:admin>cfgShow
Defined configuration
```

```
 cfg:        cfg1      ql_zone1; al_zone2; fabric_zone1; fabric_zone2

zone:       fabric_zone1
                                Fabric_ServerA; Fabric_StorageA
zone:       fabric_zone2
                                Fabric_ServerB; Fabric_StorageB
zone:         ql_zone1
                                Private_ServerA; Private_StorageA
zone:        ql_zone2
                                Private ServerB; Private StorageB
 alias: Fabric_ServerA
                                50:06:0b:00:00:06:9a:d6
 alias: Fabric_ServerB
                                50:06:0b:00:00:06:ad:10
 alias: Fabric_StorageA
                                50:06:04:82:bc:01:0a:1b
 alias: Fabric_StorageB
                                50:06:04:82:bc:01:9a:1c
 alias: Private_ServerA
                                1,3
 alias: Private_ServerB
                                1,4
 alias: Private_StorageA
                                2,2
 alias: Private_StorageB
                                2,1
 Effective configuration:
  cfg: cfg1
  zone: fabric_zone1
                          50:06:0b:00:00:06:9a:d6
                          50:06:04:82:bc:01:9a:1b
zone:      fabric_zone2
                          50:06:0b:00:00:06:ad:10
                          50:06:04:82:bc:01:9a:1c
zone:      ql_zone1
                          1,3
                          2,2
zone:    ql_zone2
                          1,4
                          2,1
test180_Jr:admin>
<END>
```

Create an Alias

An alias must be a unique alpha-numeric string beginning with an alpha character. The underscore character (_) is allowed and alias names are case sensitive. For example, `nt_hosts` is not the same name as `NT_Hosts`.

Aliases can greatly simplify the administrative process; however, they are not required to define zones.

The alias name may not exceed 64 characters.

Use the **alicreate** command to create aliases for areas 5 and 29 on switch 7.

```
test180_Jr:admin> aliCreate "alias_by_port_level", "7,
   5; 7, 29"
```

Use the **alicreate** command to create an alias for a RAID with a known WWN:

```
test180_Jr:admin> aliCreate "RAID_1_NodeName",
   "50:06:0b:00:00:06:9a:d6"
```

Definine a Zone

A zone is a group of devices that can communicate with each other. Zone membership can include ports, WWNs, aliases, or any combination of these. A device can be included in more than one zone.

To define a zone, specify the list of members to be included and assign a unique zone name; the zone name must be a unique alphanumeric string beginning with an alphabetic character. The underscore character (_) is allowed and zone names are case sensitive. For example, `green_zone` is not the same name as `Green_Zone`.

Specify zone members by port number, WWN, alias, or a combination of these.

- To specify by port number, you must specify switch domain ID and area number. For example, 2,12 indicates switch domain ID 2, area number 12. When a member is specified by port number, all devices connected to the port are included in the zone. The following is an example:

```
SW12000:admin> switchshow
switchName:     SW12000
switchType:     10.1
switchState:    Online
```

```
switchRole:     Subordinate
switchDomain:   4
switchId:       fffc04
switchWwn:      10:00:00:60:69:80:1f:42
switchBeacon:   OFF
blade1: Beacon: OFF
blade2: Beacon: OFF

Area Slot Port Gbic Speed State
=====================================
  0    1    0   id    1G   Online    E-Port
   10:00:00:60:69:80:14:f6 "12K-6" (upstream)
  1    1    1   id    N1   Online    F-Port
   21:00:00:e0:8b:05:35:51
  2    1    2   id    N2   Online    E-Port
   10:00:00:60:69:80:06:f3 "12K-6" (Trunk master)
  3    1    3   id    N2   No_Light
  4    1    4   id    N2   No_Light
  5    1    5   id    N2   No_Light
  6    1    6   id    N2   No_Light
  7    1    7   id    N2   No_Light
  8    1    8   id    N2   No_Light
  9    1    9   id    N2   No_Light
 10    1   10   id    N2   No_Light
 11    1   11   id    N1   Online    F-Port
   20:00:00:e0:69:c0:2c:b3
 12    1   12   id    N2   No_Light
.
.
.
.
SW12000:admin>
SW12000:admin>
SW12000:admin> zonecreate "testZone1","4,11"
SW12000:admin>
SW12000:admin> cfgshow
.
.
.
zone:  testZone1
                4,11
```

- To specify by WWN, specify node name or port name as an eight hex number separated by colons, for example, `10:00:00:00:60:69:00:8a`. These eight numbers are compared to the node and port name presented in a login frame (`FLOGI` or `PLOGI`).

When a zone member is specified by node name, all ports on the device are included in the zone. When a zone member is specified by port name, only that port on the device (node) is included in the zone.

- To specify by alias, specify the alias name.

Zone members can also be designated by a combination of these methods. For example, the following zone definition:

```
2,12; 2,14; 10:00:00:60:69:00:00:8a; nt_hosts
```

contains any devices connected to switch 2, ports 12 and 14, the device with a node name, or port name of `10:00:00:60:69:00:00:8a` as well as devices associated with the alias `nt_hosts`.

The above example represents a soft zone, since it contains both ports and WWNs in the same zone.

Defining a Zone Configuration

A zone configuration is a group of zones that are enforced whenever that zone configuration is enabled. A zone can be included in more than one zone configuration.

To define a zone configuration, specify the list of zones to be included and assign a zone configuration name; the zone configuration name must be a unique alphanumeric string beginning with an alphabetic character. The underscore character (_) is allowed and zone names are case sensitive. For example, `configuration1` is not the same name as `Configuration1`.

Use the `cfgcreate` command to create your zone configuration.

```
test180_Jr.admin> cfgCreate "cfg1", fabric_zone1;
  fabric_zone2"
```

Analyze the Zone Configuration

After creating and saving a zone configuration, EMC recommends analyzing the zone configuration. Doing this will save time and potential issues.

The Zoning Configuration Analyze screen displays a summary of the saved configuration and warns of the zoning conflicts before enabling them. Some of the potential errors that might be caught are:

- Ports/WWN/devices that are part of the selected configuration but are not part of the fabric.
- Zones with a single zone object.

To access the Zoning Configuration Analysis screen, select the **Analyze Config** button, which is available in the Zone Administration window in Web Tools.

Enabling a Zone Configuration

When a zone configuration is enabled, all zones within the configuration are enabled. All devices within an enabled zone are visible to each other; however, they cannot communicate outside their zone. Zones can overlap within a zone configuration.

Use the `cfgenable` to enable and save your configuration.

```
test180_Jr:admin>cfgEnable "cfg1"

Committing configuration...done.
zone config "cfg1" is in effect
```

When a zone configuration is enabled, the following happens:

1. All aliases are expanded.
2. Inconsistencies are checked. If inconsistencies are discovered, an error occurs and the previous state of the fabric is preserved. (For example, if zoning is disabled, it remains disabled; if an existing configuration is enabled, it remains enabled.)
3. Switch hardware is loaded with the zoning information.
4. Zone members are loaded.
5. Registered State Change Notifications (RSCNs) are generated.

Implementing Zoning on an Existing Fabric

The fact that zoning is already implemented eliminates the first step of creating and configuring a zone. The next step of creating aliases and zones then adding them to the existing configuration is the same. It is acceptable to have overlapping zones. In fact, it would be expected that the single HBA zones overlap one or more of the existing zones. After the single HBA zones have been put in place, the previous zones can be removed. After the previous zones are removed, the aliases that are no longer needed may also be removed. Carefully executed, this will be non-disruptive to the devices on the fabric. There may be a momentary disruption of data flow when the new zoning configuration is enabled due to the RSCN. Properly configured devices will handle this without issue.

Modifying Configurations

To make changes to an existing configuration, add, delete, or remove individual elements to create the desired configuration. Once the changes have been made, save the configuration. This ensures the configuration is permanently saved in the switch and it also ensures that the configuration is replicated throughout the fabric.

The switch configuration file can also be uploaded to the host for archiving and it can be downloaded from the host to all switches in the fabric.

Adding a Switch

When a new switch is added to the fabric, it automatically takes on the zone configuration information from the fabric. To add the new switch, attach the E_Ports and the new switch is incorporated into the fabric and the enabled zone configuration.

A new switch is a switch that has not previously been connected to a fabric with a zoning configuration. A switch that is configured for zoning may be returned to this new switch state by using the `cfgClear` and `cfgSave` commands before connecting to the fabric, or use `cfgDisable` if there is an effective configuration.

Adding a New Fabric

Adding a new fabric that has no zone configuration information to an existing fabric is very similar to adding a new switch. All switches in the new fabric inherit the zoning configuration data. If a zone configuration is in effect, then the same configuration becomes the enabled configuration. The `cfgShow` command will display the same information on all switches in the newly formed Fabric. Before the new fabric can merge successfully, it must pass the merging and segmentation criteria described in the following sections.

Before Merging Zones

To facilitate merging, check the following before merging switches or fabrics.

- **Zoning licenses** - All switches must have a Zoning license enabled.
- **Native operating mode** - All switches must be in the native operating mode.

- **Secure Fabric OS** - Do any of the switches have Secure Fabric OS? If one switch has EMC Connectrix Secure Fabric OS enabled, all switches in the fabric must have Secure Fabric OS. Refer to the *EMC Support Matrix* for more information.

  For EMC Connectrix switches, please check the EMC Support Matrix and firmware release notes for information regarding support of Secure OS.

Merging and Segmentation

The fabric is checked for segmentation during the fabric configure/reconfigure during power-up or when a switch is disabled/enabled, or when a port switches to an F-port.

The entire Defined Configuration is merged with adjacent switches, before the Effective Configuration Name is sent, if one exists.

Two databases are used with zoning. The first database is the zone configuration database. This is the data displayed as the defined configuration in the `cfgShow` command. It is stored in flash by the `cfgSave` command. This database is a replicated database, which means that all switches in the fabric will have copy of this database. When a change is made to the defined configuration, the switch where the changes were made must close its transaction for the change to get propagated throughout the fabric.

If debugging is required, the local login data can be viewed using the `portLoginShow s/p` command, where `s/p` is the slot/port number for that switch. The cache of remote logins can be viewed by making a query to the Name Server or using zoneCheck with two valid DIDs, then use the `cfgRemoteShow` command.

Merging Rules

Observe the following rules when merging zones.

Rule 1

If the local and adjacent zone database configurations are the same, they will remain unchanged after the merge.

Rule 2

If there is an effective configuration between two switches, the zone configuration in effect must be the same for the fabrics to merge.

Rule 3

If a zoning object has the same name in both the local and adjacent defined configurations, the object types and member lists must also be the same to merge. When comparing member lists, the content and order of the members are important.

Rule 4

If a zoning object appears in an adjacent defined configuration, but not in the local defined configuration, the zoning object is added to the local defined configuration. The modified zone database must be small enough to fit in the flash area allotted for the zone database.

Rule 5

If a local defined configuration is modified because of a merge, the new zone database is propagated to other the switches within the merge request.

Merging Two Fabrics

Both fabrics have identical zones and the same is configuration enabled. The two fabrics will join to make one larger fabric with the same zone configuration across the newly created fabric.

If the two fabrics have different zone configurations, they will be merged. If the two fabrics cannot join, the ISL between the switches will be segmented. Refer to Table 2-2 on page 2-13 for more information.

Merging with a v4.1.0 Fabric

If the user has an ED-12000B-based fabric, or other switches running EMC Connectrix Fabric OS V4.1.0, the firmware can operate in the same fabric with DS-32B2 and ED-12000B series switches running Fabric OS 3.0.1a or later firmware. Switches running EMC Connectrix Fabric OS V4.1.0 firmware can operate in the same fabric with all DS-16B2 series switches running v2.6.1 or later.

Merge Conflicts

When a merge conflict is present, a merge will not take place and the ISL will segment. Below is a list of possible reasons for merge conflicts.

Use the `switchshow` command to obtain additional information about possible merge conflicts, as many non-zone related configuration parameters may cause conflicts

If the fabrics have different zone configuration data, the two sets of zone configuration data are merged if possible. If the zones cannot

merge, the inter-switch link (ISL) will be segmented. A merge is not possible if any of the following exist:

Configuration mismatch	Zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.
Type mismatch	The name of a zone object in one fabric is used for a different type of zone object in the other fabric.
Content mismatch	The definition of a zone object in one fabric is different from the definition of zone object with the same name in the other fabric.

If the order of zoneset members between two switches are not listed in the same order, the configuration is considered a mismatch, resulting in the switches being segmented in the fabric. For example: `cfg1 = z1; z2` is different from `cfg1 = z2; z1`, even though members of the configuration are the same. If zoneset members between two switches have the same name defined in the configuration, make sure zoneset members listed are in the same order.

Splitting a Fabric

If the connections between two fabrics are no longer available, the fabric will segment into two separate fabrics. Each new fabric will retain the same zone configuration.

If the connections between two fabrics are replaced and no changes have been made to the zone configuration in either of the two fabrics, then the two fabrics will merge back into one single fabric. If any changes that cause a conflict have been made to either zone configuration, then the fabrics may segment.

Zone Merging Scenarios

Table 2-3 provides information on merging zones and the expected results.

Table 2-3 Zone Merging Scenarios

Description	Switch A	Switch B	Expected Results
Switch A with a defined configuration **Switch B** does not have a defined configuration	defined: cfg1: zone1: ali1; ali2 effective: none	defined: none effective: none	Configuration from **Switch A** to propagate throughout the fabric in an inactive state, since the configuration is not enabled.
Switch A with a defined and enabled configuration **Switch B** does has a defined configuration but no effective configuration	defined: cfg1 zone1: ali1; ali2 effective: cfg1:	defined: cfg1 zone1: ali1; ali2 effective: none	Configuration from **Switch A** to propagate throughout the fabric.
Switch A and **Switch B** have the same defined configuration. Neither have an enabled configuration.	defined: cfg1 zone1: ali1; ali2 effective: none	defined: cfg1 zone1: ali1; ali2 effective: none	No change (clean merge).
Switch A and **Switch B** have the same defined and enabled configuration	defined: cfg1 zone1: ali1; ali2 effective: cfg1:	defined: cfg1 zone1: ali1; ali2 effective: cfg1:	No change (clean merge).
Switch A does not have a defined configuration **Switch B** with a defined configuration	defined: none effective: none	defined:cfg1 zone1: ali1; ali2 effective: none	**Switch A** will absorb the configuration from the fabric.
Switch A does not have a defined configuration **Switch B** with a defined configuration	defined: none effective: none	defined:cfg1 zone1: ali1; ali2 effective: cfg1	**Switch A** will absorb the configuration from the fabric. With cfg1 as the effective cfg.

Table 2-3 Zone Merging Scenarios *(continued)*

Description	Switch A	Switch B	Expected Results
Switch A and **Switch B** have the same defined configuration. Only **Switch B** has an enabled configuration.	defined: cfg1 zone1: ali1; ali2 effective: none	defined: cfg1 zone1: ali1; ali2 effective: cfg1	Clean merge - with cfg1 as the effective cfg.
Switch A and **Switch B** have different defined configurations. Neither have an enabled zone configuration.	defined: cfg2 zone2: ali3; ali4 effective: none	defined: cfg1 zone1: ali1; ali2 effective: none	Clean merge - the new cfg will be a composite of the two -- defined: cfg1 zone1: ali1; ali2 cfg2: zone2: ali3; ali4 effective: none
Switch A and **Switch B** have different defined configurations. **Switch B** has an enabled configuration.	defined: cfg1 zone2: ali3; ali4 effective: none	defined: cfg1 zone1: ali1; ali2 effective: cfg1	Clean merge - The new cfg will be a composite of the two. With cfg1 as the effective cfg.
Effective cfg mismatch	defined: cfg1 zone1: ali1; ali2 effective: cfg1 zone1: ali1; ali2	defined: cfg2 zone2: ali3; ali4 effective: cfg2 zone2: ali3; ali4	Fabric segments due to: Zone Conflict cfg mismatch.
cfg content mismatch	defined: cfg1 zone1: ali1; ali2 effective: irrelevant	defined: cfg1 zone1: ali3; ali4 effective: irrelevant	Fabric segments due to: Zone Conflict content mismatch.
	defined: cfg1 zone1: ali1; ali2 effective: irrelevant	defined: cfg1 zone1: ali1; ali4 effective: irrelevant	Fabric segments due to: Zone Conflict content mismatch.
Same content - different effective cfg name	defined: cfg1 zone1: ali1; ali2 effective: cfg1 zone1: ali1; ali2	defined:cfg2 zone1: ali1; ali2 effective:cfg2 zone1: ali1; ali2	Fabric segments due to: Zone Conflict cfg mismatch.

Table 2-3 Zone Merging Scenarios *(continued)*

Description	Switch A	Switch B	Expected Results
Same content - different zone name	defined: cfg1 zone1: ali1; ali2 effective: irrelevant	defined: cfg1 zone2: ali1; ali2 effective: irrelevant	Fabric segments due to: Zone Conflict content mismatch.
Same content - different alias name	defined: cfg1 ali1: A; B effective: irrelevant	defined:cfg1:ali2: A; B effective: irrelevant	Fabric segments due to: Zone Conflict content mismatch.
Same name - different types	effective: zone1: MARKETING	effective: cfg1: MARKETING	Fabric segments due to: Zone Conflict type mismatch.
Same name - different types	effective: zone1: MARKETING	effective: alias1: MARKETING	Fabric segments due to: Zone Conflict type mismatch.
Same name - different types	effective:cfg1: MARKETING	effective:alias1: MARKETING	Fabric segments due to: Zone Conflict type mismatch.

Resolving Zone Conflicts

Zone conflicts can be resolved by using the `configupload` command and performing a cut and paste operation so the config info matches in both fabrics being merged.

Zone conflicts can also be resolved by using the `cfgclear` command followed by the `cfgdisable command` on the incorrectly configured segmented fabric, followed by a `portDisable/portEnable` command on one of the ISL ports that connects the fabrics. This will cause a merge making the fabric consistent with the correct configuration.

CAUTION

Be careful in using the cfgclear command. It will delete the defined Zoning database.

Rules of Zoning Architecture

Observe the following rules when configuring zones.

Rule 1

Type of Zoning (Hard or Soft) - If security is a priority, Hard zoning is recommended.

Rule 2

The use of aliases is optional with zoning. Using aliases requires structure when defining zones. Aliases will aid administrators of zoned fabric in understanding the structure and context.

Rule 3

Evaluate the security requirements of the fabric. If additional security is required, add Secure Fabric OS into the fabric.

Rule 4

Inter-operability Fabric - If the fabric includes an ED-12000B or DS-32B2 and the user is supporting a third-party switch product, they will only be able to do WWN zoning. Other types of zoning, including QuickLoop, will not be supported.

Rule 5

Evaluate if the fabric will have QuickLoop Fabric Assist (QLFA) or QuickLoop (QL) in it. If the user is running Fabric OS v4.1.0, consider the following before creating and setting up QLFA zones:

QuickLoop Zoning

QuickLoop/QuickLoop zones cannot run on switches running Fabric OS v4.1.0. However, Fabric OS v4.1.0 can still manage (create, remove, update) QL zones on any non-v4.1.0 switch.

QuickLoop Fabric Assist

Fabric OS v4.1.0 cannot have a Fabric Assist host directly connected to it. However, Fabric OS v4.1.0 can still be part of a Fabric Assist zone if a Fabric Assist host is connected to a non-v4.1.0 switch.

Rule 6

Testing a (new) zone configuration. Before implementing a zone, the user should run the Zone Analyzer from Web Tools to isolate any possible problems. This is especially useful as fabrics increase in size

Rule 7

Zone changes in a production fabric can result in a disruption of I/O under conditions where an RSCN is issued as a result of a zone change and the HBA is unable to process the RSCN fast enough. Though RSCNs are a normal part of a functioning SAN, the pause in I/O may not be acceptable. For these reasons, it is recommended to perform zone changes only when the resulting behavior is predictable and acceptable. Changing HBA drivers can rectify the situation.

Rule 8

After changing or enabling a zone configuration, the user should confirm that the nodes and storage are able to identify and access one another. Depending on the platform, the user may need to reboot one or more nodes in the fabric with the new changes.

3

Using QuickLoop Zones

This chapter contains the following information:

Overview

In addition to Zoning fabrics, explained in Chapter 2, Zoning can also be used to zone QuickLoop, allowing arbitrated loops to be attached to a fabric. The QuickLoop and Zoning combination allows a private host to fully participate in a storage area network (SAN). By partitioning selected devices within a QuickLoop into a QuickLoop zone you can enhance management of a Fibre Channel Arbitrated Loop (FC-AL) in a legacy environment.

QuickLoop Zones

QuickLoop zones are hardware enforced. Switch hardware prevents unauthorized data transfer between ports within the zone allowing devices to be partitioned into zones to restrict system access to selected devices. When devices are included in a zone, they are visible only to other devices within that zone.

QuickLoop zone members are designated by looplet (port number), or by Arbitrated Loop Physical Address (AL_PA). There are 126 unique AL_PAs per QuickLoop; therefore, a QuickLoop zone can contain no more than 125 devices.

Each QuickLoop port uses one AL_PA.

Fabric zones and QuickLoop zones are independent of each other; both types of zones can co-exist in the same zone configuration and QuickLoop devices can be included within a fabric zone configuration. But, while devices within a QuickLoop can be seen by a public host, devices within each QuickLoop are only visible to devices within their separate QuickLoop environment.

In QuickLoop zoning, devices within a QuickLoop can be partitioned off within that QuickLoop to form QuickLoop zones; in other words, a QuickLoop Zone is a subset of a QuickLoop and can include only QuickLoop devices.

QuickLoop is supported in Fabric OS v3.1, however, it is not supported in Fabric OS v4.1.0.

QuickLoop Zoning Advantages

In addition to the advantages of fabric zoning - security, customized environments, and optimization of IT resources - QuickLoop zoning can protect devices from disruption by unrelated devices during a critical process, for example, during a tape backup session.

In a QuickLoop with zoning enabled, transmission of the loop initialization primitive (LIP) signal and loop initialization are controlled by the switch; the LIP is transmitted only to looplets within the affected zone; other looplets on the QuickLoop are not affected. In this way, unwanted disruption to devices can be controlled.

Configuring QuickLoop Zones

To configure QuickLoop zoning, perform the following:

- Create a QuickLoop
- Define a QuickLoop Zone
- Define a QuickLoop Zone Configuration

Create a QuickLoop

To create a QuickLoop with zoning, the `qloopcreate` command is used. The `qloopcreate` command allows the user to reference up to two switch WWN for a QuickLoop. This will create a qloop in the zoning definition, which is referenced in the config to make the QuickLoop effective. When using zoning to manage QuickLoop, qloops must be defined and present in the config.

Define a QuickLoop Zone

A QuickLoop zone is a group of L_ports or AL_PAs that can communicate with each other. These ports and AL_PAs must reside within the same QuickLoop. To be a QuickLoop zone, every member must be either a looplet (L_port) or an AL_PA within a single QuickLoop. QuickLoop zones can overlap looplets, but they must be confined to a single QuickLoop.

QuickLoop zones are hardware enforced, but zones within a single looplet are not enforceable; therefore, it is recommended that you do not partition devices within a looplet into different zones.

To define a QuickLoop zone, first enable and create the necessary QuickLoops. Then specify the list of members to be included and assign a unique zone name. A QuickLoop zone name must be a unique alpha-numeric string beginning with an alpha character. The underscore character (_) is allowed and zone names are case sensitive. For example, Zone1 is not the same name as zone1.

To create a QuickLoop zone specify QuickLoop zone members by looplet, by AL_PA, or by combination of the two.

To Specify by Looplet:

Specify the QuickLoop zone name, in quotes, and the physical ports to be included, in quotes.

Example

```
Zonecreate "QLZoneName", "0,0; 0,1; 2,6; 2,7; 2,8"
```

To specify by AL_PA:

Specify the QuickLoop zone name, in quotes, with the QuickLoop name, and desired AL_PAs in quotes. All AL_PAs must be associated with a QuickLoop name.

Example

```
Zonecreate "QLZoneName", "qloop1[01,02,04,e0,e1,e2]"
```

To specify a combination of looplet and AL_PA:

Example

```
   Zonecreate "QLZoneName", "0,2; 0,3;
   qloop1[ca,cb,e1,e2]"
```

Define a QuickLoop Zone Configuration

To define a QuickLoop zone configuration, assign a zone configuration name and specify the QuickLoop zones to be included, by zone name. The QuickLoop names of the QuickLoop zones must also be included in the zone configuration.

An example of a QuickLoop zone configuration is:

```
cfgname "cfgname", "QLZoneName"
```

Example

```
cfgname "QLconfig_1", "QLZoneName",
   "qloop1[01,02,04,e0,e1,e2]"
cfgenable "QLconfig_1"
```

QuickLoop Fabric Assist

Fabric Assist allows a private host to communicate with public/private targets located anywhere within the fabric (if no zoning exists). Private hosts and targets are put into a single Fabric Assist Zone, and are identified either by domain and port number or by WWN. Each Fabric Assist zone can have only one private host. The user will need QuickLoop and Zoning licenses to use these features.

Fabric Assist Zone Setup

Zoning commands with the prefix "`fazone`" that mirror other zoning commands are listed below: `fazoneCreate`, `fazoneAdd`, `fazoneDelete`, `fazoneRemove`, and `fazoneShow`.

Private hosts are indicated within a fazone or alias by "H{}". Within a single fazone or alias, multiple initiators are detected during zone creation process. `CfgEnable` can fail if multiple initiators are found in a single fazone.

Fabric Assist Zone Creation

The private host within a fazone has its own AL_PA domain space. A target that is zoned with multiple hosts may be given different AL_PAs. A max of 125 unique targets may be zoned with private hosts on any given switch.

A fazone private host must be the only node on a loop. Sharing a loop with other nodes will cause the fazone to fail.

Fabric Assist Operation

When "cfg" is enabled, AL_PAs are created for all zoned targets that are online, on the private host's loop. The private host's loop is re-LIPed so that it may "see" any added AL_PAs.

As additional targets join the fabric, if they are within the fazone, they will have an AL_PA created on the private host's loop. This is triggered off of the RSCN. A target may be zoned with one or more private hosts, and will have a unique AL_PA created on each host's loop.

LIP Propagation

LIPs are propagated to all private devices within a fazone. They are not sent to public targets in the fazone. LIPs are only sent when a fazone target comes online. A loop of fazone targets that are re-LIPed, but do NOT add any new targets will not propagate a LIP to any private hosts.

Fabric Assist Debugging

The `FaDebugShow` command can help troubleshoot FA issues by displaying internal Fabric Assist tables.

`FaDebugShow:` Displays the internal Fabric Assist tables.

A

Zoning Concepts and Guidelines

This appendix provides the following information on zoning concepts and guidelines:

Storage Area Networks

The storage area network introduces the connectivity of networks to the SCSI protocol. The Fibre Channel standard provides for up to 16 million devices attached to the network. The change in scale requires a new method to locate the devices on the fabric, so that access can be accomplished in an acceptable time frame.

The well known fabric service "name server" was implemented to address this need. When a device initially accesses the fabric it must perform a login process. During this process the device will register with the name server. The name server records information about the device i.e. protocols supported, World Wide Name (WWN), network address, supported class of service, etc.

When an initiator accesses the network it can query the name server for all attached devices and their capabilities. Any initiator can query (probe) the fabric for all targets. And then proceed to initialize the targets and perform I/O. If another initiator is already using the target and has stored data on it as with a disk or tape. Data may be lost.The process of zoning is used to provide a virtual SCSI bus that limits the devices that an initiator can discover and access.

Zoning

Zoning acts as a filter that is applied by the name server against the query from the initiator that limits the information returned by the name server to the initiator. A zone contains the WWN of the initiator and the WWN of any devices that it is allowed to access. When an initiator queries the name server for accessible devices in the fabric, the name server will look for all zones that contain the WWN of the initiator. Then a list is formed from all the members of the zones and is applied to the contents of the name server. Only devices that are in the list and in the name server are returned to the initiator as accessible devices. The initiator then uses the list of returned devices along with the access parameters returned and proceeds to further inquire of the devices for specific operational capabilities.

Devices that are not part of the zone are not returned as accessible devices. It is important to note that this process does not prohibit access to the device. If the initiator has prior knowledge of the device, it can access the device. The name server does not control access to devices on the fabric. Dependable zoning operation depends on the cooperation of all devices in the fabric to only access devices that are returned in the query from the name server. EMC Connectrix fabric switches provide for hardware enforcement of the zoning configuration to prevent unwanted access to devices.

Devices can be listed in more than one zone. Thus overlapping zones are permitted. A concept of most permissible access is used in zoning. When an initiator requests the list of accessible devices, if at least one zone containing the WWN of the initiator exists then any device in that zone is accessible. If the same device exists in another zone that does not contain the WWN of the initiator, the device is still accessible to the initiator.

Zone Configuration Management

Management of the zone information is provided via command line (Telnet), Web Tools, and Fabric API via third party software. The zone information has three components: the zone object(s), the zone name, and the zone configuration. One or more objects (devices) are placed into a zone and given a zone name. One or more zone names are placed into a zone configuration. One or more configurations are defined. Then one and only one configuration is made the effective configuration for the fabric. The number of aliases, zones, and defined configurations is limited only by the memory available in the EMC Connectrix switch.

It is important to note that zone configuration is managed on a fabric basis. Zoning configuration data is automatically (by closing the transaction) distributed by the Fabric OS to all switches in the fabric, preventing a single point of failure for zone information. The zoning configuration can be administered from any switch.

Zoning Implementations

Zoning can be enabled on the host, in the switch fabric, and in most storage units. Storage units typically implement LUN based zoning, commonly referred to as LUN masking. Fabric switches will implement name server-based zoning where the zone member are identified by WWN or port location in the fabric. Host-based zoning can implement WWN or LUN masking.

Host-based Zoning

Host-base zoning requires the host configuration to be correct so that zoning conflicts are avoided. This provides a greater opportunity for administrative errors to allow conflicting access to targets. The zoning interface varies from host operating systems, even among different HBA vendors. This increases the opportunity for administrative errors to occur. If a host is not configured with the zoning software, it can access all devices in the fabric resulting in the possibility of data corruption.

Storage-based Zoning

Storage-based zoning is usually referred to as LUN masking. Its basic function is to limit access to the LUNs on the storage port to specific WWN of the server HBA. This form of zoning is needed in most SANs. It functions during the probe portion of the SCSI initialization. The server will probe the storage port for a list of available LUNs and their properties. The storage system will compare the WWN of the requesting HBA to the defined zone list. It will then return the LUNs that are assigned to the WWN. Any other LUNs on that storage port will not be made available to the server.

Fabric-based Zoning

Fabric-based Zoning is commonly referred to as name server-based or soft zoning. With EMC Connectrix switches there may also be additional hardware enforcement of the zone, refer to *Hardware Enforced Zoning in a Connectrix Fabric* on page A-10. When a device makes a query to the fabric name server, the name server determines which zone(s) the device belongs to. It then returns to the requesting device information on all members of the zone(s) that are present in the fabric. Devices in the zone are identified by World Wide node name, World Wide port name, or domain/port of the switch the device is connected to.

Fabric Based Zoning Forms

This is perhaps the most controversial aspect of zoning. There are a number of approaches for the implementation of fabric zoning. All will work in most cases. However, there are pros and cons to each form. The primary forms are: no fabric zoning, single HBA, grouping by operating system, grouping by application, and port allocation.

Zoning by Application

In most environments, the concern for availability is by application, not by server, such as in clusters. Zoning by application will most likely require zoning multiple operating systems into the same zones. Some operating systems have issues co-existing in the same zone with other operating systems. This method of zoning creates the possibility that a minor server in the application suite potentially has the ability to disrupt a major server. An example is a web server being able to disrupt a data warehouse server. Zoning by this method may also result in a zone with a large number of members that would provide a greater opportunity for administrative errors to occur, such as Registered state change notification (RSCNs) may go out to a larger group than might be necessary.

Zoning by Operating System

Zoning by operating system has issues similar to zoning by application. In a large site, this zone may become very large and complex. When zone changes are made they typically do not involve a particular server type, but are more concerned with applications. Situations have been encountered with operating system clusters. If members of different clusters can see storage assigned to another cluster, they may attempt to own the other cluster's storage and compromise the stability of the clusters.

Zoning by Port Allocation

Zoning can be done based on switch port rather than the WWN of the device. This provides some security to the fabric, but requires very solid processes to prevent the incorrect device type of zoning being attached to the wrong ports. Zoning by port allocation should be avoided unless the administration team has very rigidly enforced processes for port and device allocation in the fabric. It does however provide some positive features. For instance, when a storage port, server HBA, or tape drive is replaced, the change of WWN for the new device is of no consequence. As long as the new device is connected to the original port, it will continue to have the same access rights. The ports on the edge switches can be pre-associated to

storage ports and control of the fan-in ratio can be established. With this technique, the administrative team could not overload any one storage port by associating too many servers with it.

Zoning by Single HBA

Zoning by single Host bus adapter (HAB) most closely recreates the original SCSI bus. Each zone created has only one HBA (initiator) in the zone. Then each of the target devices the initiator should access is added to the zone. Typically, a zone would be created for the HBA and the disk storage ports would be added. If the HBA accesses tape devices, a second zone is created with the HBA and associated tape devices in it. In the case of clustered systems, it may be appropriate to have an HBA from each of the cluster members included in the zone. This is equivalent to having a shared SCSI bus between the cluster members. This presumes that the clustering software provides a methodology to manage access to the shared devices.

In a large fabric, this does require the creation of possibly hundreds of zones. However, each zone would only contain a few members. Zone changes would affect the smallest possible number of devices. The impact of an incorrect zone change would be minimized. This zoning philosophy is the preferred method.

The Effect of Zoning on RSCN Delivery

Whenever a change occurs in the name server, such as a device addition or removal from the fabric, a state change notification (RSCN) must be generated. In the absence of zoning, an RSCN is sent to all devices on the fabric. Each device should then query the name server to determine how the membership of the fabric has changed. This will happen even if the device change does not affect the other devices. In large fabrics, this can result in a significant amount of traffic being generated, although typically for only short time.

For instance, if a new initiator joins the fabric, there is little purpose in notifying all the other initiators of the change. Initiators do not typically communicate with each other. An equivalent situation exists with targets. As targets generally do not communicate with each other, they have little use in being notified of the addition or removal of another target.

After zoning has been implemented, only affected devices in the changed zone will receive the RSCN. If devices are already aware of their zoned members, then they will not receive an RSCN. Only devices that are affected by the change will receive an RSCN. While all devices are supposed to handle RSCN traffic without affecting normal operation, experience has shown that this is not always the case. Thus, the overall stability of the fabric is increased when zoning is implemented. Table A-1 provides additional information.

Table A-1 RSCN Delivery

External Events	Connectrix FOS v2.x up to v2.5	Connectrix FOS v3.0	Connectrix FOS v2.6/3.0.2/4.0	Connectrix FOS 3.1/4.1.0
Fabric reconfigure with no domain change	Fabric RSCN to all devices	Fabric RSCN to all devices	No RSCN	No RSCN
Switch disable	Fabric RSCN to all devices	Fabric RSCN to all devices	Domain RSCN to zoned devices only	No RSCN
Switch enable	Fabric RSCN to all devices	Fabric RSCN to all devices	No RSCN	No RSCN

Table A-1 RSCN Delivery (continued)

External Events	Connectrix FOS v2.x up to v2.5	Connectrix FOS v3.0	Connectrix FOS v2.6/3.0.2/4.0	Connectrix FOS 3.1/4.1.0
Device power up	Device RSCN to zoned devices only	Aggregated[a] RSCN to zoned devices only	Aggregated RSCN to zoned devices only	Aggregated RSCN to affected zoned devices only
Device shutdown	Device RSCN to zoned devices only	Aggregated RSCN to zoned devices only	Aggregated RSCN to zoned devices only	Aggregated RSCN to affected zoned devices only
Zone change	Fabric RSCN to all devices	Fabric RSCN to all devices	Fabric RSCN to all devices	Fabric RSCN to affected devices only
Switchname/IP Address change	Domain RSCN to all devices	Domain RSCN to all devices	Domain RSCN to all devices	Domain RSCN to all devices

a. Aggregated RSCN combines multiple device RSCNs into one.

Deviations from Single HBA Zoning

There are cases when the need will arise to deviate from the single HBA zoning. Such as clustered systems, SAN Management appliances, and when initiators must communicate with each other because another protocol like IP is being utilized. When this need arises proper consideration of all ramifications of the deviation must be understood.

Important EMC strongly recommends testing in a non-production environment.

Hardware Enforced Zoning in a Connectrix Fabric

Zoning employs the name server to limit the information returned to an initiator in response to a name server query. This is referred to as **soft zoning**. If an initiator has knowledge of the network address of a target device, it does not need to query the name server to access it. This allows for undesired access to a target device with the potential for data corruption. EMC Connectrix switches augment the name server zoning with hardware enforcement. Name server or soft zoning is always active whenever a zone configuration is in effect. However, certain conditions determine when hardware enforcement will be active.

When hardware enforced or **hard zoning** is active, the Connectrix switch will monitor the communications and block any frames that do not comply with the effective zone configuration. This blocking is performed at the transmit side of the port where the destination device is located. A zone configuration will typically be comprised of many zones, and the hardware enforcement decision is made on a per zone basis. The exact methodology varies on different switch models. The use of hardware enforcement is decided by the Fabric OS whenever the fabric membership or zone configuration changes.

Zone definitions:

- **Domain/Port zone** - All members of this zone are specified with domain/port pairs only. Area values may be used when zoning on an ED-12000B.
- **WWN zone** - All members of this zone are specified with WWN numbers only. They may be node or port versions of the WWN.

- **MIXED zone** - This zone contains members specified by either domain/port or WWN, and it contains at least one member specified by each method.
- **Overlapping zones** - Two or more zones that contain a common member. The member may be specified by domain/port or WWN.

DS-8B, DS-16B Series Switch Model Fabrics

The Connectrix DS-8B and DS-16B series switch enables hardware enforced zoning only on Domain/Port zones. Any WWN or mixed zones will not be hardware enforced. Any Domain Port zone that overlaps with a MIXED or WWN zone will not be hardware enforced.

An overlap will occur when a member specified by WWN is connected to a port in a Domain/Port zone. The Domain/Port zone will lose its hardware enforcement, even though a review of the zone configuration would not indicate this.

DS-16B2, DS-32B2, and ED-12000B Series Switch Model Fabrics

DS-16B2, DS-32B2, and ED-12000B series switches enable hardware enforced zoning on Domain/Port zones and WWN zones. Overlap of like zone types will not result in the loss of hardware enforcement. Overlap with another zone type will result in the loss of hardware enforcement. As in the DS-16B2 witches, connecting a device specified by WWN into a port specified in a Domain/Port zone will result in loss of the hardware enforcement in both zones.

DS-8B, DS-16B, DS-16B2, DS-32B2, and ED-12000B Series Switch Model Fabrics

In mixed fabrics, each switch type continues to enable hardware enforcement of zoning according to the conditions established above. The challenge is that the administrator must now know which switch type the device is attached to in order to determine if hardware enforcement will be active. This is accomplished using the command `portzoneshow`.

Best Practices for Hardware Zone Enforcement

When a site policy has been established requiring hardware enforcement, it certainly is desired that the hardware enforcement always occur. From the preceding paragraphs, it should be clear that there are cases when determining the applicability of hardware enforcement can be difficult. Three basic cases have simple rules for assuring that hardware enforcement is used.

Rule 1

For DS-8B and DS-16B series switch fabrics, always use Domain/Port identifiers only. Never identify a zone member by WWN.

Rule 2

For DS-16B2, DS-32B2 and ED-12000B series switch fabrics chose to use either WWN or Domain/Port zones. See section Zone Enforcement for additional information when choosing zones.

Rule 3

For mixed fabrics always preferably use Domain/Port identifiers. If it is desired to use WWN identifiers, the following methodology may be used. Always place disk, tape units (targets) on the DS-16B2, DS-32B2, and ED-12000B series switches, and use WWN zoning only. If all the targets are on the DS-16B2, DS-32B2, and ED-12000B series switches, hardware enforced zoning will be active to protect them. This does not hardware protect the initiators, but in general they do not offer resources anyway and will reject any probe attempt by other initiators.

B

Zoning and Secure Fabric OS

This appendix contains the following information on Zoning and Secure Fabric OS:

Using Zoning to Administer Security

Zones can be used to provide controlled access to fabric segments and to establish barriers between operating environments. Zones are used to isolate systems with different uses or protect systems in a heterogeneous environment, for example; when Zoning is in secure mode, merge operations do not occur.

Connectrix Zoning is done on the primary Fabric Configuration Server (FCS). The primary FCS switch makes zoning changes and other security related changes. The primary FCS switch also distributes zoning to all other switches in the secure fabric. All existing interfaces can be used to administer zoning.

Zone management operations must be performed from the primary FCS switch using a zone management interface, such as telnet or Web Tools. A zoning database can be altered, provided you are connected to the primary FCS switch.

When two secure fabrics join, the traditional zoning merge does not occur. Instead, a zoning database is downloaded from the primary FCS switch of the merged secure fabric. When E_ports are active between two switches, the name of the FCS server and a zoning policy set version identifier are exchanged between the switches. If the views of the two secure fabrics are the same, the fabric's primary FCS server downloads the Zoning database and Security policy sets to each switch in the fabric. If there is a view conflict, the E_ports are segmented as incompatible security data.

Secure Fabric OS requires the activation of an EMC security license.

As part of Zoning Architecture, the user will need to determine which of the two basic Zoning Architectures will work best for their fabric. With time and planning, the basic hard zone configuration will work for most sites. If a site has additional security needs, the user will need to add the additional layer of Secure Fabric OS to lock down the fabric, in addition to the standard Zoning Architecture.

C

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure C-1).

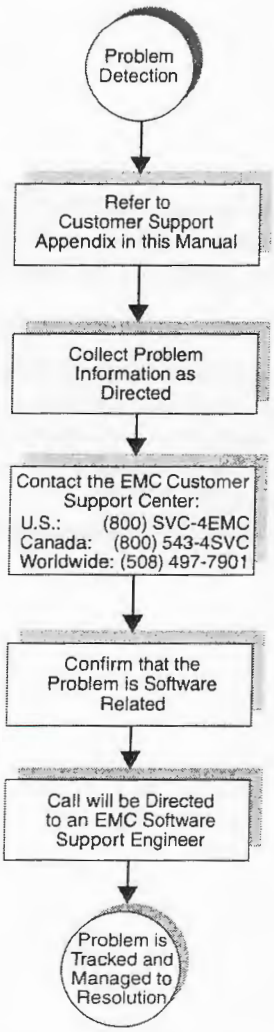


Figure C-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

```
http://powerlink.EMC.com
```

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode.*

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit.*

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL.*

M

Media See *Transceiver.*

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port.*

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A Brocade product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

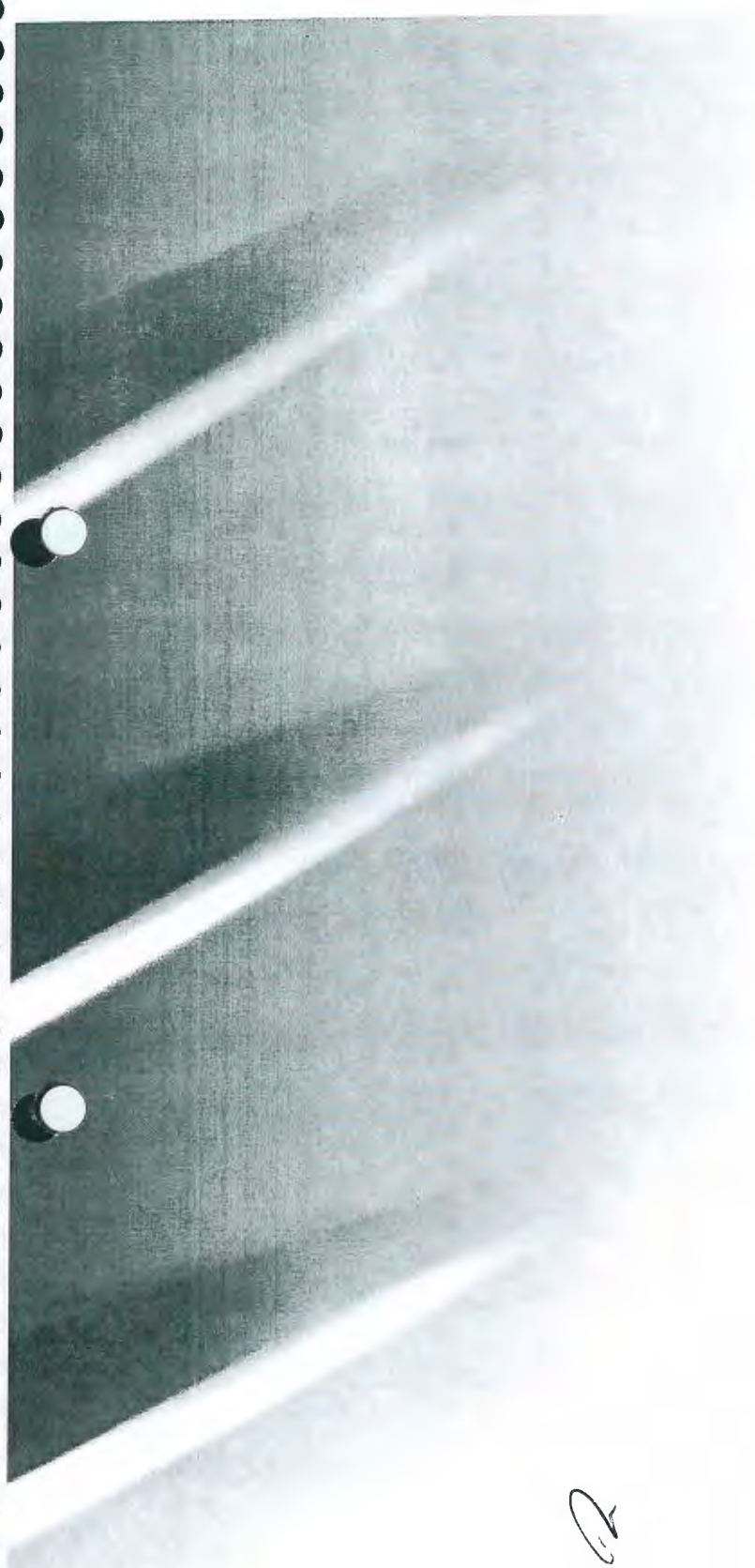
Index

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ECT 21623 CPL-AC

ANEXO SWITCH TIPO 03
PARTE 9

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br



EMC Connectrix B Series
Extended Fabric
Version 3.1 and Version 4.1

USER GUIDE

P/N 300-000-646
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

Connectrix B Series systems have been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Preface

The EMC Connectrix B Series Extended Fabric User Guide provides information for installing the Extended Fabric license and how to use Extended Fabric. It is supported on the DS-16B2, DS-32B2, and ED-12000B running any EMC qualified version of Fabric OS. This Guide is part of EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B documentation set.

The EMC Connectrix B Series Extended Fabric provides information on Extended Fabric that you may encounter during installation and operation of the DS-16B2, DS-32B2 and ED-12000B.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch and Enterprise Director. For the most up-to-date information on product features, see your product release notes.

If a feature in the DS-16B2, DS-32B2, or ED-12000B does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

Readers of this guide are expected to be familiar with the Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B operating environment.

Organization

Here is an overview of where information is located in this guide.

- Chapter 1, *Introducing Connectrix B Series Extended Fabric*, provides an overview of extended fabrics.

- Chapter 2, *Installing Extended Fabric*, provides instructions for installing Extended Fabric on DS-16B2, DS-32B2, and ED-12000B switches.
- Chapter 3, *Using Extended Fabric*, provides information to configure ports to support long distance links through Telnet or through Web Tools.
- Appendix A, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix Departmental Switch DS-16B2, DS-32B2 and Enterprise Director ED-12000B.
- The *Glossary* defines terminology used in this manual.

Related Documentation

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-16B2 QuickLoop Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*

- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the warning.

Typographical Conventions

EMC uses the following type style conventions in this guide:

Palatino, bold	◆ Dialog box, button, icon, and menu items in procedures ◆ Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	User entry. For example: **`symmpoll -p`**
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.emc.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

`http://powerlink.emc.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to **`techpub_comments@emc.com`** with your opinions of this guide.

1 Introducing Connectrix B Series Extended Fabric

EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B Extended Fabric (hereafter referred to as Extended Fabric) allows you to use Fibre Channel technology to create a fabric interconnected at a distance of up to 100 km.

Support for distances greater than 100 km may be available for certain applications and configurations. Support parameters for extended distance solutions, such as those around DWDM technology, can be obtained from the EMC Support Matrix. Please note that the information found in the EMC Support Matrix specifies support parameters around connectivity. You should work closely with EMC field personnel and professional services to determine whether application requirements will be met over these extended distances.

This chapter introduces you to Extended Fabric.

Overview

You can use Extended Fabric technology to create a fabric interconnected at a distance of up to 100 km or more. Extended Fabric can increase the allowable distance between two switches. It is an optionally licensed product that runs on Connectrix DS-16B2, DS-32B2, and ED-12000B switches with any EMC qualified version of Fabric OS.

Extended Fabric optimizes the internal buffering algorithm. Extended Fabric provides maximum buffering between E_Ports connected over an extended distance through buffer reconfiguration. This results in line-speed performance of close to full Fibre Channel speed for switches interconnected at 100 km or more, thus providing the highest possible performance for transfers between switches. The fibre channel connection extensions can be provided by Wave Division Multiplexing (WDM) devices.

Performance may vary depending on the condition of the fiber-optic connections between the switches. Losses due to splicing, connectors, tight bends, and other degradation can affect the performance over the link and the maximum distance possible.

To enable Extended Fabric, you must install the Extended Fabric license on each switch connected via the extended link.

If a fabric is created exclusively using DS-16B2, DS-32B2, and ED-12000B switches, the long distance extended fabric configuration has to be set only once for each fabric at the edge port connector switch. The edge port connector switch automatically works with the rest of the switches in the fabric.

To enable Extended Fabric, each switch in the fabric must be configured individually. For the non-edge switches, this is a configuration setting and there is no requirement to purchase the Extended Fabric license.

Figure 1-1 on page 1-3 shows the Switch Information tab.

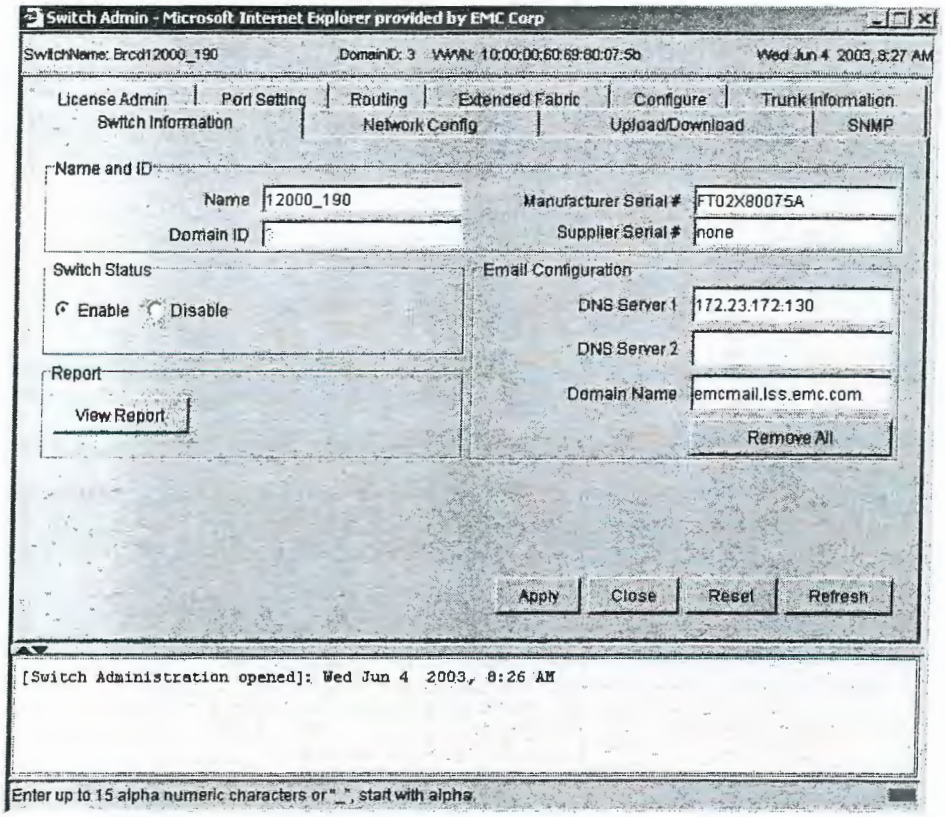


Figure 1-1 Switch Information Tab

2 Installing Extended Fabric

Installing Extended Fabric involves the installation of a license on each switch that has long-distance links. Contact your EMC sales representative to obtain a transaction key. This transaction key can be converted into a license key by going to the following website:
`http://powerlink.emc.com`

You can install Extended Fabric either through Telnet or through Web Tools.

Installing Extended Fabric Through Telnet

To install EMC Connectrix B Series Extended Fabric through Telnet:

1. Log on to the switch through Telnet using an account that has administrative privileges (refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric OS Reference Guide* or the *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Guide).*

2. To determine whether the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Extended Fabric license is already installed on the switch, enter **`licenseShow`** on the Telnet command line.

   A list appears showing all the licenses currently installed on the switch.

```
SB5_12000B_0:admin> licenseShow
RRRebbzzQSSSfcA:
    Fabric license
bbbdQRQ99mcceR4:
    Web license
    Zoning license
    Fabric Watch license
    Trunking license
R99ySdbb99WAAzTY:
    Extended Fabric license
    Performance Monitor license
SB5_12000B_0:admin>
```

   If the EMC Connectrix Extended Fabric license is not included in the list, proceed to Step 3. If it is correctly listed, the license is already installed and immediately available.

3. Enter the following on the command line:

   `licenseAdd key`

   where `key` is the license key provided to you, surrounded by double quotation marks. The license key is case sensitive and must be entered exactly as given.

4. Verify the license was added by entering the following on the command line:

   `licenseShow`

If the EMC Connectrix B Series Extended Fabric license is listed, the feature is installed and immediately available. If the license is not listed, repeat Step 3.

Installing Extended Fabric Through Web Tools

To install EMC Connectrix B Series Extended Fabric through Web Tools:

1. Launch the web browser by entering the switch name or IP address in the **Location/Address** field, and press ENTER.

   Web Tools launches, displaying the Fabric View.

2. Click on the **Admin View** icon on the relevant switch panel.

   The Logon window appears.

3. Enter a logon name and password with administrative privileges and press ENTER.

   The Administration View displays.

4. Click the **License Admin** tab (Figure 2-1 on page 2-5), enter the license key in the **License Key** field, and click **Add License**.

   The Extended Fabric feature is available as soon as the license key is added.

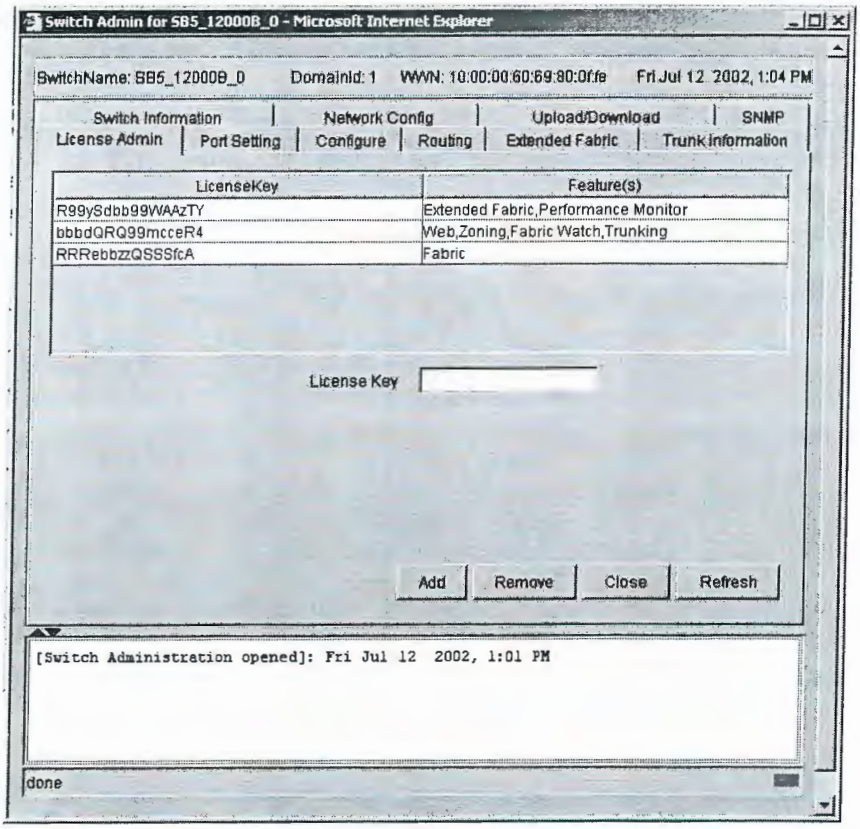


Figure 2-1 License Admin Tab

3 Using Extended Fabric

This chapter describes the supported configurations that you can use to create Extended Fabrics, and provides instructions on how to create Extended Fabrics. You can configure ports to support long-distance links through Telnet or through Web Tools. For information about using Web Tools to configure ports, refer to the *EMC Connectrix Departmental Switch DS-32B2* and *Enterprise Director ED-12000B Web Tools User Guide* or the *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*.

This chapter provides the following information:

Overview

The Extended Fabric feature achieves long distance connections by allocating more frame buffers for Fibre Channel traffic. Long distance connections require more frame buffers than regular ISL connections. The greater the distance level of a ISL long distance connection, the more frame buffers are required. This affects the amount of buffers left over in the quad. A quad is defined as a group of four adjacent ports that share a common pool of frame buffers. In a Connectrix switch (or port card in the ED-12000B), ports 0 - 3 belong to a single quad, ports 4 - 7 belong to a single quad, and so on.

Since the total number of frame buffers is limited in quad when one port in a quad is configured as a long distance port, all remaining ports in the same quad must be configured appropriately. Refer to the Long Distance Port Matrix in Table 3-1 on page 3-9.

Configuring Extended Fabric

To use Extended Fabric, the following parameters must be set:

- Switch configuration to enable long distance
- Port configuration to select the long-distance mode

Supported Configuration

An Extended Fabric can consist of:

- Connectrix DS-8B/16B switches only
- Connectrix DS-16B2 switches only
- Connectrix DS-32B2 and ED-12000B switches only
- A combination of Connectrix DS-8B/16B, DS-16B2, DS-32B2, and ED-12000B switches

In a combination configuration, the long-distance ISL that connects the fabric can only be installed between edge port switches containing the same ASIC type, i.e. ,DS-16B2, or DS-32B2 and ED-12000B switches. An Extended Fabric does not work if the long-distance ISL is installed between edge port switches with nonmatching ASIC types. Long-distance ISLs between DS-8B/DS-16B cannot be connected to switches DS-16B2, DS-32B2, and ED-12000B. Refer to Figure 3-1 for more information.

The long distance extended fabrics configuration needs to be set only once for each fabric at the edge switch E-port. The configuration should be between switches with the same ASIC (refer to above note). Long distance ports consume more buffers than regular ISL ports, which means that a long distance port could disable other ports in the same quad due to lack of buffers. Refer to the *Long Distance Port Matrix* on page 3-9 for buffer credit information.

Trunking is only supported with L0 mode.

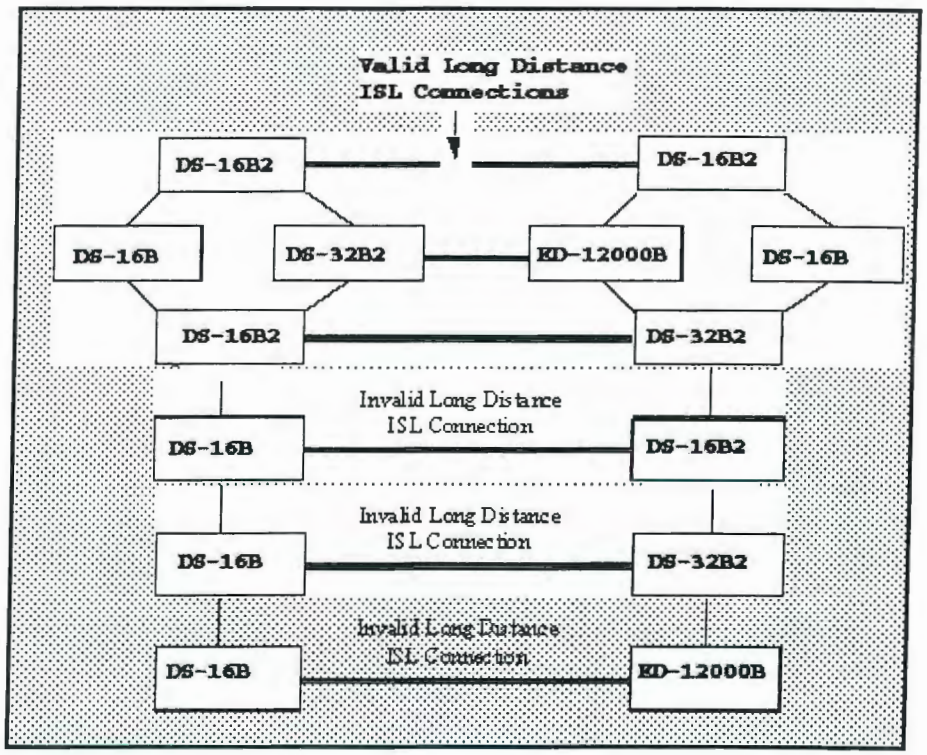


Figure 3-1 Extended Fabric Configurations

Long distance between DS-16B and DS-16B2, DS-16B and DS-32B2, or DS-16B and ED-12000B ports is NOT supported when Long Distance Fabric Parameter is set.

Support for distances greater than 100 km may be available for certain applications and configurations. Support parameters for extended distance solutions, such as those around DWDM technology, can be obtained from the EMC Support Matrix. Please note that the information found in the *EMC Support Matrix* specifies support parameters around connectivity. You should work closely with EMC field personnel and professional services to determine whether application requirements will be met over these extended distances.

Configuring an Extended Fabric Connection

If the fabric contains one or more switches running Fabric OS v2.x or v3.0.x or the switch has a long distance ISL, the following parameters need to be set to configure Extended Fabrics.

- Port configuration: the long distance fabric parameter set to 1
- Switch configuration must be set to enable long distance - **on switches running FOS 2.x**

The long distance ISL ports must have the same configuration or the fabric will be segmented.

If one switch in the fabric has the long distance fabric parameter set to 1, all switches in the fabric must have the parameter set to 1. Otherwise the fabric will be segmented

---

Trunking is supported for normal E_Ports (referred to as L0 in the `portcfglongdistance` command) up to 5 km at the full speed permitted by the link. ISL Trunking is only supported with the L0 `portcfglongdistance` mode. For information about these modes and Extended Fabrics in general, refer to the *EMC Connectrix B Series ISL Trunking User Guide*.

Enabling Long Distance on a DS-8B and DS-16B Series Switch

In the DS-16B2 switches, only the ISL long-distance switches need to have the long distance mode enabled.

To set the long-distance fabric mode bit:

1. Log in to the switch using Telnet.

CAUTION

This is an offline command. I/O will cease while performing this operation.

2. Enter `switchDisable`.
3. Enter `configure`.
4. Enter `yes` or `y` at the Fabric parameters line.

5. Press **ENTER** to scroll through the Fabric parameters without changing their values until you reach the **Long Distance Fabric** parameter.
6. Enter `1` on the following Telnet line:

```
Long Distance Fabric [0]: 1
```

Example

```
switch:admin> switchdisable
switch:admin> configure

Configure...

Fabric parameters (yes, y, no, n): [no] yes

    Domain: (1..239) [3] 5
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0] 1
    BB credit: (1..16) [16]

  Virtual Channel parameters (yes, y, no, n): [no]
  Zoning Operation parameters (yes, y, no, n): [no]
  RSCN Transmission Mode (yes, y, no, n): [no]
  NS Operation Parameters (yes, y, no, n): [no]
  Arbitrated Loop parameters (yes, y, no, n): [no]
  System services (yes, y, no, n): [no]
  Portlog events enable (yes, y, no, n): [no]
Committing configuration...done.

switch:admin>
```

Configuring Long Distance on a DS-16B2, DS-32B2, and ED-12000B Series Switch

To configure long distance fabric mode on a DS-16B2, DS-32B2, and ED-12000B series switch:

Only active SFPs should be used when using Extended Fabric.

Trunking is only supported with L0 mode.

This procedure is used to configure the ports in a long distance ISL connection. Both ports must be configured to the same distance level.

To configure the distance level for a Extended Fabric ISL port:

1. Login to the switch as the admin user.
2. Issue the following command:

```
portcfglongdistance [slot/]port
[distance_level] [vc_translation_link_init]
```

where:

slot	Specify the slot number in an ED-12000B switch. The slot number must be followed by a slash (/) and the port number.
port	Specify the port number where you want to initiate the long distance ISL port.
distance	This indicates the long distance mode to be set on the port.

Example The example shows a configuration for the distance level.

```
switch:admin> portcfglongdistance 1/1 LD 1
done.
switch:admin>
```

To set the port configuration:

Issue the `portCfgLongDistance` command to view the current port level.

Possible levels for a port are:

LX = Any of L0, L1, L2, LE, L0.5 and LD.

L0 = Represents an Extended Fabric mode of 10 kilometers for a 1 Gb switch and 5 kilometers for a 2 Gb switch.

Level 0 does not require an Extended Fabric license.

LE = Represents an Extended Fabric mode of 10 kilometers for a 2 Gb switch.

Level E does not require an Extended Fabric license.

L1 = Represents an Extended Fabric mode of 50 kilometers for a 1 Gb and a 2 Gb link.

Level 1 requires an Extended Fabric license.

L2 = Represents an Extended Fabric mode of 100 kilometers for a 1 Gb link, and 50 kilometers for a 2 Gb link.

Level 2 requires an Extended Fabric license.

Level 0.5 (L05) = Supports up to 25 km for 1 G and 2 G. This mode does not support trunking with other ports.

Level D (LD) (Dynamic long distance configuration) = LD mode dynamically assigns buffers based on the link round trip timing calculation. Ports will be disabled once the buffer pool has been depleted. For example, if two ports are configured at LD and each is connected at 100 km, all buffers will be utilized and the remaining two ports will be disabled.

3. Repeat step 2 for the remote long distance ISL port. Both the local and remote long distance ISL ports must be configured to the same distance level for the connection to work. When the connection is initiated, the fabric will reconfigure.

VC Translation Mode

The VC Translation mode is used to initiate long distance connections.

`VC_Translation_Link_Init`	Specify **1** to activate long distance link initialization sequence. This mode is used to initiate long distance connections. When configuring a long distance connection, the first port configured does not require this mode. When configuring the second port of a connection, use this mode to initiate communication between the ports.

Long Distance Port Matrix

Certain buffers are dedicated for each port, and others are shared among the ports. In Extended Fabric mode, one port is given an increase of dedicated buffers from this pool.

Since the total number of frame buffers in a quad is limited, the following Extended Fabric port matrix introduces a combination of long distance ports that are available, as shown in Table 3-1. Ports A, B, C, and D are the four consecutive ports in a quad. A quad is the group of ports managed by an ASIC.

Table 3-1 Long Distance Port Matrix

Fabric OS	Speed	Port a	Port b	Port c	Port d
v3.0 and v 4.0	1 Gb/s	L2	L1/E	Fx/LE	x
	1 Gb/s	L2	Fx/LE	Fx/LE	Fx/LE
	1 Gb/s	L1/E Fx	L1/E Fx	L1/E Fx	L1/E Fx/LE
v3.0 and v 4.0	2 Gb/s	L2	Disabled	Disabled	Disabled
	2 Gb/s	L1	L1/E /LE	Disabled	Disabled
	2 Gb/s	L1	E/LE	E/LE/ Fx	Disabled
	2 Gb/s	L1	Fx	Fx	Fx
	2 Gb/s	E/LE/ Fx	E/LE/ Fx	E/LE/ Fx	E/LE/ Fx
v/ 3.1 and v 4.1	1 Gb/s	L2	E/L1	LE/L0.5/Fx	Disabled
	1 Gb/s	L2	L0.5	LE/L0.5/Fx	Disabled
	1 Gb/s	L2	L0.5	LE/Fx	LE
	1 Gb/s	L2	LE/Fx	LE/Fx	LE/Fx
	1 Gb/s	E/L1/L0.5/LE/Fx	E/L1/L0.5/LE/Fx	E/L1/L0.5/LE/Fx	E/L1/L0.5/LE/Fx
	1 Gb/s	LD	LD	LD	LD

Table 3-1 Long Distance Port Matrix *(continued)*

Fabric OS	Speed	Port a	Port b	Port c	Port d
v. 3.1 and 4.1	2 Gb/s	L2	E	Fx	Disabled
	2 Gb/s	L2	LE/Fx	LE/Fx	Disabled
	2 Gb/s	L2	L0.5	Disabled	Disabled
	2 Gb/s	L1	L1	Disabled	Disabled
	2 Gb/s	L1	E	E/LE/Fx	Disabled
	2 Gb/s	L1	LE/Fx	LE/Fx	Fx
	2 Gb/s	L1	L0.5	LE/Fx	Disabled
	2 Gb/s	L0.5	L0.5	L0.5	Disabled
	2 Gb/s	L0.5	E/L0.5/LE/Fx	E/LE/Fx	Disabled
	2 Gb/s	L0.5	E/L0.5/LE/Fx	LE/Fx	LE/Fx
	2 Gb/s	L0.5	E/LE/Fx	E/LE/Fx	LE/Fx
	2 Gb/s	E/LE/Fx	E/LE/Fx	E/LE/Fx	E/LE/Fx
	2 Gb/s	LD	LD	LD	LD

Short Wavelength Optics Supports distances of up to 500 m at 1 Gb/s and 300 m at 2 Gb/s.

BB Credits Allocated Per Port Type

1 G - Fx = Standard port w/ 16 BB Credits

1 G - E = Level 0 E_Port w/ 27 BB Credits

1 G - LE = Level E E_Port w/ 13 BB Credits

1 G - L1 = Level 1 E_Port w/ 27 BB Credits

1 G - L2 = Level 2 E_Port w/ 60 BB Credits

2 G - Fx = Standard port w/ 16 BB Credits

2 G - E = Level 0 E_Port w/ 27 BB Credits

2 G - LE = Level E E_Port w/ 19 BB Credits

2 G - L1 = Level 1 E_Port w/ 54 BB Credits

2 G - L2 = Level 2 E_Port w/ 108 BB Credits

There are a total of 108 buffers per quad, which can be allocated by ports within the ASIC. In any quad, the port long-distance setting is limited to available buffers from the buffers mentioned above.

Setting the Extended Fabric Port Configuration

You can configure a port to support long-distance links by using `portCfgLongDistance`.

portCfgLongDistance

Configures a port to support long-distance links.

Syntax v4.1 `portCfgLongDistance [slotnumber/]portnumber[, distance]`

Availability admin

Description Use this command to specify the allocation of enough full size frame buffers on a particular port to support a long-distance link of up to 100 km. The port is used as an E_Port. The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

When this command is invoked without the optional operand, you are prompted to enter the long-distance level number. As shown in Table 3-2, the level value must be one of the following:

Table 3-2 Long-Distance Level Values for the portCfgLongDistance Command

Level	Effect
L0	Reconfigures port as a normal switch port. (This option supports up to 10km links for 1 G, or 5 km links for 2 G.)
LE	Level E mode is for E_ports for distances beyond 5 km and up to 10 km especially for 2 G link speeds. LE does not require Extended Fabric license.
L1	Level 1 long distance, up to 50 km.
L2	Level 2 long distance, up to 100 km.
L05	Supports up to 25 km for 1 G and 2 G.
LD	Dynamically assigns buffers based on the link round trip timing calculations.

When a port is configured to be a long-distance port, the output of `portShow` and `switchShow` displays the long-distance level. In the `portShow` output, the long-distance level is indicated as "`medium`" for

level 1 long distance, and "`long`" for level 2 long distance. In the `switchShow` output, the format is `Lx`, where *x* is the long-distance level number, except for level 0, which is not displayed in `switchShow`.

Operands This command has the following operands:

The slot number only applies to ED-12000B.

`slotnumber`	Specify the slot number in ED-12000B switches. The slot number must be followed by a slash and the port number. The ED-12000B have a total of 10 slots counted from 1 to 10. Slots 5 and 6 are control processor cards, and slots 1through 4 and 7 through 10 are switch cards. On each blade card there are 16 ports counted from the bottom 0 to 15. A particular port must be represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). This operand is not required for switches that do not have blades.
`portnumber`	Specify a port number. Valid values for port number vary depending on switch type. This operand is required.

distance This operand indicates the distance to the connected port. This operand is required. The valid values for this operand are:

L0 = Reconfigure port to be regular switch port.

This option supports up to 10 km links for 1 G, or 5 km links for 2 G.

LE = Level E mode is for E_ports for distances beyond 5 km and up to 10 km, for 2 G link speeds.

LE does not require extended fabric license.

L1 =Level one long distance (up to 50 km).

L2 = Level two long distance (up to 100 km).

L05 = Supports up to 25 km for 1 G and 2 G.

LD = (Dynamic long distance configuration) Dynamically assigns buffers based on the link round trip timing calculation.

A quad is defined as a group of four adjacent ports that share a common pool of frame buffers. Ports 0 through 3 belong to a quad, ports 4 through 7 belong to a quad, and so on.

Example The following example is for a 100 km link on a port in an ED-12000B:

```
switch:admin> portCfgLongDistance 2/3, L2
   done
```

This example is for the ED-12000B only.

In a combination configuration, the long-distance ISL that connects the fabric can only be installed between edge port switches containing the same ASIC type, i.e., DS-16B2, or DS-32B2 and ED-12000B switches. An Extended Fabric does not work if the long-distance ISL is installed between edge port switches with nonmatching ASIC types. Long-distance ISLs between DS-8B/DS-16B cannot be connected to switches DS-16B2, DS-32B2, and ED-12000B. Refer to Figure 3-1 on page 3-4 for more information.

A

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure A-1).

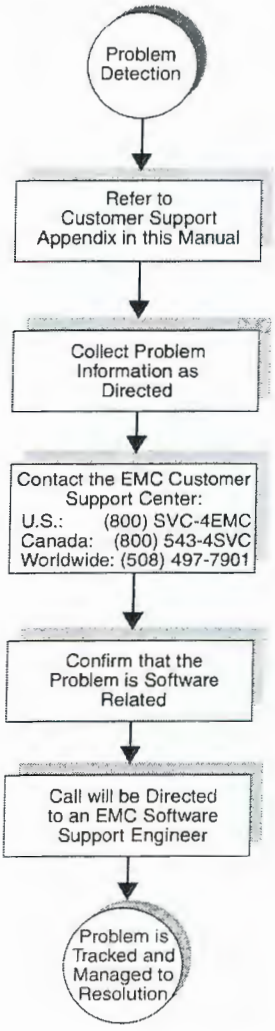


Figure A-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

```
http://powerlink.emc.com
```

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 Bit error rate. 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM

gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode*.

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit*.

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL*.

M

Media See *Transceiver*.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port*.

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A Brocade product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector, DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

Index

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – MANUAL VOLUME 10

2003
PASTA 38

Figures

Figures

Tables

Tables

Preface

The EMC Connectrix Model ED-12000B Hardware Reference Manual provides information for installing the ED-12000B and is intended to assist you in the installation and use of ED-12000B. This manual is part of EMC Connectrix Model ED-12000B documentation set.

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix. For the most up to date information on product features, see your product release notes.

If a feature in the ED-12000B director does not function properly or does not function as described in this manual, please contact the EMC Customer Support Center for assistance.

Audience

Readers of this manual include anyone who must install, configure, or operate the ED-12000B.

Organization

Here is an overview of where information is located in this manual.

- Chapter 1, *Introducing the ED-12000B Switch*, provides an overview of the EMC Connectrix Model ED-12000B director.
- Chapter 2, *Starting and Operating the ED-12000B Switch*, provides instructions for basic director operation and explains how to interpret system activity.
- Chapter 3, *Configuring the ED-12000B Switch*, provides instructions for initial start up and configuration of the ED-12000B director.
- Chapter 4, *Maintaining the ED-12000B Switch*, provides instructions for director maintenance.

- Appendix A, *Product Specifications for the ED-12000B*, describes components, physical specifications, environment and other facility requirements, switch memory, and standards compliance for the ED-12000B.
- Appendix B, *Product Specifications for the EC-1230B* describes components, physical specifications, environment, and other facility requirements, switch memory, and standards compliance for the EC-1230B cabinet.
- Appendix C, *Troublshooting and Diagnostics*, includes information on troubleshooting the ED-12000B and diagnostic tests.
- Appendix D, *Setting Up and Installing Modems*, discusses the location of components, and how to connect modems to the ED-12000B, set up a remote modem system, and verify the modem connection.
- Appendix E, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix Model ED-12000B.
- The *Glossary* provides explanations for terminology used in this manual.

Related Documentation

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Fabric Watch Reference Manual*
- *EMC Connectrix B Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Zoning Reference Manual*
- *EMC Connectrix B Extended Fabrics User Guide*
- *EMC Connectrix B Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Performance Monitoring User Guide*
- *EMC Connectrix DS-32B2 Hardware Reference Manual*

Conventions Used in this Manual

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this manual:

Palatino, bold	◆ Dialog box, button, icon, and menu items in text ◆ Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	◆ User entry. For example: **`symmpoll -p`** ◆ Options in command line syntax
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.emc.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink Web site at:

`http://powerlink.emc.com`

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to `techpub_comments@emc.com` with your opinions of this manual.

1 Introducing the ED-12000B Switch

This chapter provides the following information:

Overview

The ED-12000B is a high-performance core switch for large storage area networks, available in configurations ranging from 32 to 128 ports (two 64 port switches in a single chassis). It can operate as the only switch in a fabric or in a fabric containing multiple switches. The ED-12000B includes Fabric OS version 4.1.

High availability features include:

- Two redundant hot-swappable control processor (CP) cards with automatic failover
  - One CP card actively manages the ED- 12000B, and the other acts as a standby to allow failover if required.
  - Failover occurs automatically if the active CP card fails
  - The CP cards can be replaced while the ED-12000B is operating if one CP card is replaced at a time
- Non-disruptive firmware download for Fabric OS v4.1.0 and later
- Up to eight hot-swappable 16-port cards
- Four hot-swappable power supplies
- Three hot-swappable blower assemblies (two required for adequate cooling)
- WWN card that is hot-swappable in Fabric OS v4.1.0 and later
- Two redundant AC inputs, each of which suplies power to the entire chassis

The Fibre Channel ports support link speeds of 1 and 2 Gb/s (inbound and outbound), and automatically negotiate to the highest common speed of all devices connected to the port. They are compatible with short wave-length and long wave-length SFP (small form factor pluggable) transceivers, universal and self-configuring, and capable of individually becoming FL_Ports (fabric loop ports), F_Ports (fabric ports), or E_Ports (expansion ports).

The ED-12000B is 14 rack units in height, and has an air-cooled chassis.

Port Side of Chassis

The fibre channel ports support link speeds of 1 and 2 Gb/s (inbound and outbound), and automatically negotiate to the highest common speed of all devices connected to the port. They are compatible with short wave-length and long wave-length SFP (small form factor pluggable) transceivers, universal and self-configuring, and are capable of individually becoming FL_Ports (fabric loop ports), F_Ports (fabric ports), or E_Ports (expansion ports).

Figure 1-1 shows the port side of the ED-12000B, which provides access to the following components:

- Up to 8 port cards with each card containing 16 Fibre Channel SFP ports.
- Two CP cards, each with a modem serial port, terminal serial port, and 10/100 Mbps autosensing ethernet port.
- Four power supplies that are hot-swappable and have built-in fans.
- Two AC power connectors, each with an on/off AC power switch.

For operating information for the components, refer to Chapter 2, *Starting and Operating the ED-12000B Switch*.

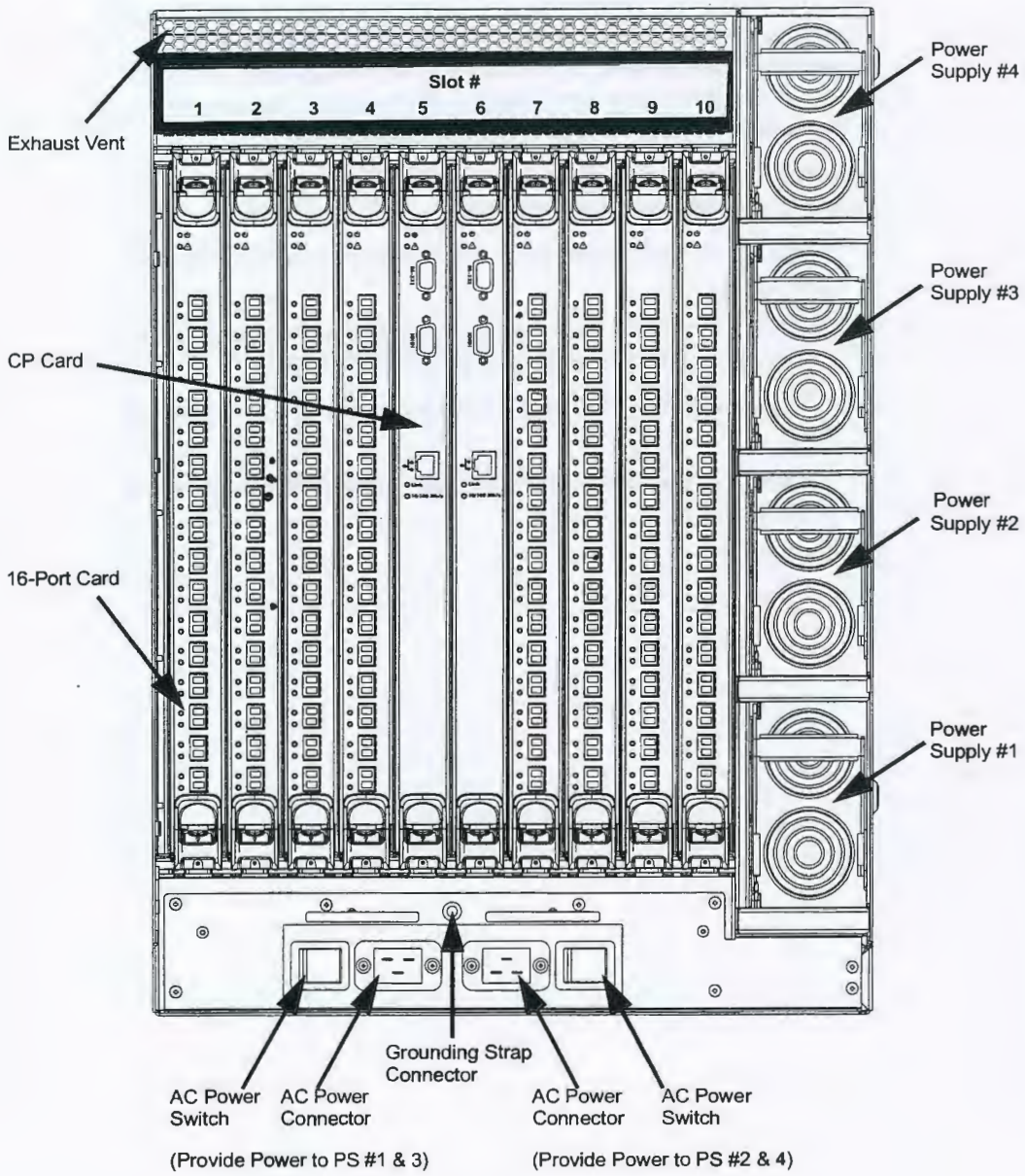


Figure 1-1 Port Side of the ED-12000B

Blower Assembly Side of Chassis

Figure 1-2 shows the blower assembly side of the ED-12000B chassis, which provides access to the following components:

- WWN card and bezel — Provide LEDs for monitoring switch from the blower assembly side and stores WWN and IP address information.
- Blower assemblies — Three blower assemblies, individually hot-swappable.

For operating information for each of the components, refer to Chapter 2, *Starting and Operating the ED-12000B Switch.*

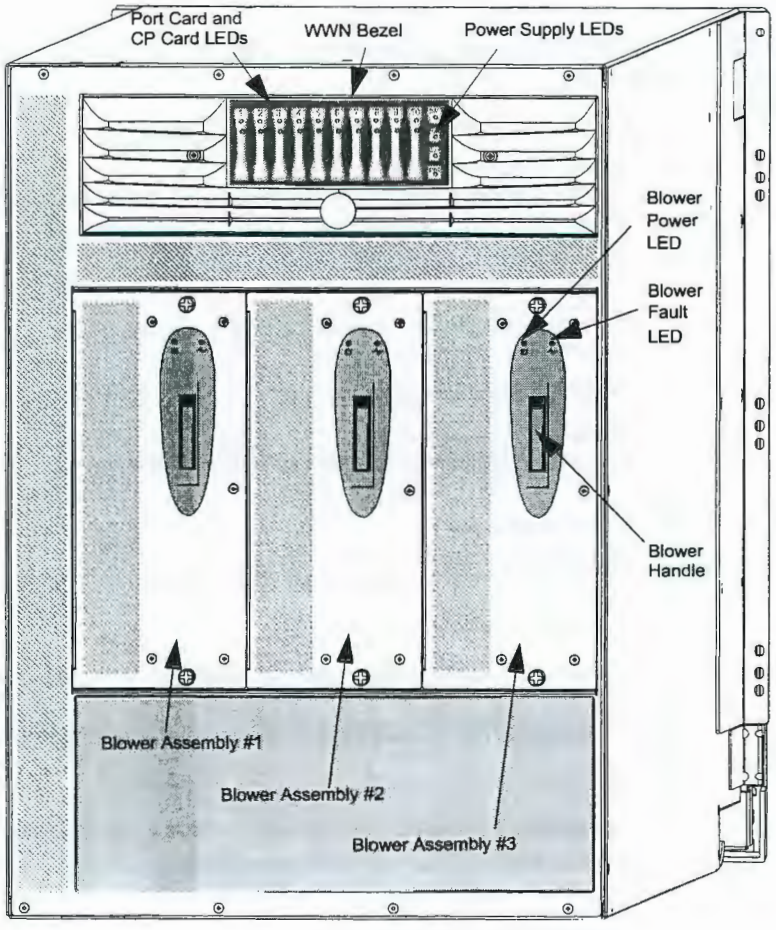


Figure 1-2 Blower Assembly Side of the ED-12000B

Monitoring and Managing the ED-12000B

The ED-12000B can be managed 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 system debugging and performance analysis.

The ED-12000B automatically performs Power-On Self Test diagnostics (POST) each time it is turned on, and any errors are recorded in the error log. For more information about POST, see *POST and Boot Specifications* on page A-15.

Management Interface Compatibility

The ED-12000B is compatible with the following management interfaces:

- Command line interface through a Telnet connection

  For more information refer to the *Fabric OS Procedures Manual.*

- Web Tools

  For more information refer to the *Web Tools User Guide.*

- SNMP Applications

  For more information refer to the *MIB Reference Manual.*

- Fabric Manager

  For more information refer to the *EMC Connectrix B Fabric Manager User Guide.*

These management methods can be used out-of-band (Ethernet).

Softare Products Supported

In addition, the ED-12000B supports the following software products:

- Web tools

  Provides a graphical interface that allows monitoring and management of fabrics and individual switches and ports from a standard workstation.

  For more information refer to the *Web Tools User Guide.*

- Zoning

  For information refer to the *Zoning Reference Manual.*

- Fabric Watch

  For information refer to the *Fabric Watch Reference Manual.*

- Performance Monitoring

  For information refer to the *Performance Monitoring User Guide.*

- Extended Fabrics

  For information refer to the *Extended Fabric User Guide.*

- ISL Trunking

  For information refer to the *ISL Trunking User Guide.*

- Secure Fabric OS

  For more information refer to the *Fabric OS Procedures Manual.*

For information about diagnostic tests and error messages, refer to the *Diagnostic and System Error Message Reference Manual.*

Check the EMC Support Matrix for the most current firmware revisions.

2 Starting and Operating the ED-12000B Switch

This chapter provides the following information:

Turning the ED-12000B On and Off

The ED-12000B is engineered for reliability and requires no routine operational steps or maintenance. This chapter provides information about the LEDs for each individual component and basic information about diagnostic tests.

The status of individual components can be determined through the LEDs (refer to *Effective Cable Management* on page 2-14), or through the CLI commands that are described in *Environmental Status and Maintenance Commands* on page 4-4.

It is also possible to set up monitoring alerts using SNMP, syslog, or Fabric Watch (if a Fabric Watch license is available). Fabric Watch alarms can be configured for each component.

Refer to the *Fabric Watch User Guide* for information about the types of alarms and how to configure them.

To turn the ED-12000B on:

Verify both power cords are connected to the AC power connectors on the front of the chassis, and flip both green AC power switches to `1`. The green AC power switches illuminate when turned on.

The ED-12000B only detects modems during power on or reboot. If a modem is connected to an operating switch, a reboot is required for the ED-12000B to detect the modem. For modem installation instructions, refer to the *ED-12000B Modem Installation Procedure*.

To turn the ED-12000B off:

Flip both AC power switches to `0`. To remove all sources of power from the switch, disconnect both cables from the power source.

Removing all power from the switch triggers a system reset. When power is restored, all devices are returned to the initial state and the switch runs POST.

CAUTION

Allow the ED-12000B to run for a minimum of 10 minutes after powering on before powering off again.

Operating Information for System Components

16-Port Cards

The ED-12000B can contain up to two logical switches, each with its own configuration: one for any 16-port cards in slots 1-4, and one for any 16-port cards in slots 7-10. The 16-port cards can be installed 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 switch can continue to operate while a 16-port card is being replaced, but any devices connected to the 16-port card must be disconnected. To ensure correct air circulation inside the switch and protection from dust, filler panels can be ordered for any empty slots.

Replacement instructions are provided under *Removing and Installing a 16-Port Card or Filler Panel* on page 4-8.

The active CP card controls both logical switches.

CAUTION

Verify port cards are operational before rebooting the port card or switch. Do not reboot the switch during port card and replacement process.

Wearing an ESD grounding strap is recommended when working 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. There are no user-serviceable parts inside the 16-port card.

CAUTION

Each 16-port card provides 16 auto-sensing Fibre Channel ports, capable of auto-sensing data transmission speeds of 1 and 2 Gb/s.

Trunking and Cabling Recommendations

The ports on each of the 16-port cards are color-coded to indicate which ports can be used in the same ISL Trunking group: four ports marked with black solid ovals alternate with four ports marked with oval outlines.

ISL Trunking is a Fabric OS feature that 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, refer to the *ISL Trunking User Guide*.

Due to wavelengths used in transmitting data, a minimum length is required for cables that connect the ED-12000B ports to device ports, as follows:

9 Microns	Single-mode (SM)	2 Meters
50 Microns	Multi-mode (M5)	2 Meters
62.5 Microns	Multi-mode (M6)	2 Meters

Determining the Status of a Port Card

To determine the status of a 16-port card:

1. Check the LED indicators on the 16-port card. Refer to Table 2-1 on page 2-18 for LED interpretation.
2. Check 16-port card status using the `slotShow` command.

For additional information about this command, refer to the *Fabric OS Reference Manual*.

Control Processor Cards

CAUTION

Wearing an ESD grounding strap is recommended when working 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. There are no user-serviceable parts inside

the CP card.

Allow POST to complete before performing a switch reboot or HA failover.

High availability is provided through redundant CP cards: an *active* CP card and a *standby* CP card. The active CP card is the one actively controlling the ED-12000B. If the active CP card fails 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.

Failover may cause a command in progress to fail; verify the correct completion of any commands that are in progress when a failover occurs. Allow POST to complete before issuing the hafailover command. Switch beaconing (synchronized flashing of LEDs) is not preserved through a failover.

Information about both CP cards, including which card is active, is available through the `haShow` command. For information about commands and whether they can be entered through the active or standby CP card, refer to the *Fabric OS Reference Manual*.

The switch can continue to operate while a CP card is being replaced.

An illustration of the CP Card is provided in Figure 2-5 on page 2-20.

Each CP card provides the following ports:

- *Modem serial port* — The modem serial port has an RS-232 connector wired as a DTE device, and is designed to connect to a 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 can be used 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 10/100 Mbps.

A separate modem can be connected to each modem serial port, and then connected to the same or separate telephone lines for redundancy.

The ED-12000B only detects modems during power on or reboot. If a modem is connected to an operating switch, the ED-12000B must be rebooted in order to detect the modem.

To ensure correct air circulation inside the switch and protection from dust, filler panels can be ordered 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
- Web Tools
- Zoning
- Secure Fabric OS
- Performance Monitoring

If Secure Mode is enabled on an ED-12000B, sectelnet or SSH sessions can be established to the IP addresses of the logical switches and the standby CP card but not to the active CP card. If the CP cards failover, any sectelnet/SSH sessions to the IP address of the standby CP card are automatically disconnected.

For EMC Connectrix switches, and for the most current firmware revisions., check the EMC Support Matrix and firmware relase notes.

Determining the Status of a CP Card

To determine the status of a CP card:

1. Check the LED indicators on the CP card. Refer to Table 2-2 on page 2-21 for LED interpretation.
2. Check CP card status using the `slotShow` and `haShow` commands.

   For additional information about these commands, refer to the *Fabric OS Reference Manual*.

Connecting Modems to the CP Cards

A separate modem can be connected to each modem serial port. The modems can then be connected to the same or separate telephone

lines for redundancy. For installation instructions, refer to *Setting Up a Remote Modem System* on page D-7.

The ED-12000B only detects modems during power on or reboot. If a modem is connected to an operating switch, the ED-12000B must be rebooted in order to detect the modem.

Operating Information for the Power Supplies

The ED-12000B uses four power supplies, with a minimum of two required to power a completely loaded chassis. The left power connector provides power to the power supplies in slots #1 and #3 (color-coded blue), and the right power connector provides power to the power supplies in slots #2 and #4 (color-coded yellow).

The ED-12000B can continue operating while a power supply is replaced if at least one power supply continues operating for every four 16-port cards installed. A minimum of two power supplies are recommended.

Determining the Status of a Power Supply

To determine the status of a power supply:

1. Check the LED indicators on the power supply. Refer to Table 2-4 on page 2-25 for LED interpretation.
2. Check power supply status using the `psShow` command. The power supply status displays **OK**, **absent**, or **faulty**. If a power supply is faulty, contact EMC technical support. For additional information about the `psShow` command, refer to the *Fabric OS Reference Manual*.

CAUTION

To protect against AC failure, EMC recommends a minimum of one power supply in slot #1 or slot #3, and one in slot #2 or #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.

Disassembling any part of the power supply voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the power supply.

AC Power Input Connectors and AC Power Switches

The ED-12000B has two AC power input connectors, each with a green AC toggle switch. The left power input connector provides power to the power supplies in slots #1 and #3, and the right power input connector provides power to the power supplies in slots #2 and

#4. The power input connectors and their associated power supplies are color-coded.

CAUTION

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 ED-12000B and are specific to the country in which the system is installed. The AC power switches light up green when on.

Figure 2-4 shows the AC panel and the retainers used to prevent accidental disconnection of the power cords.

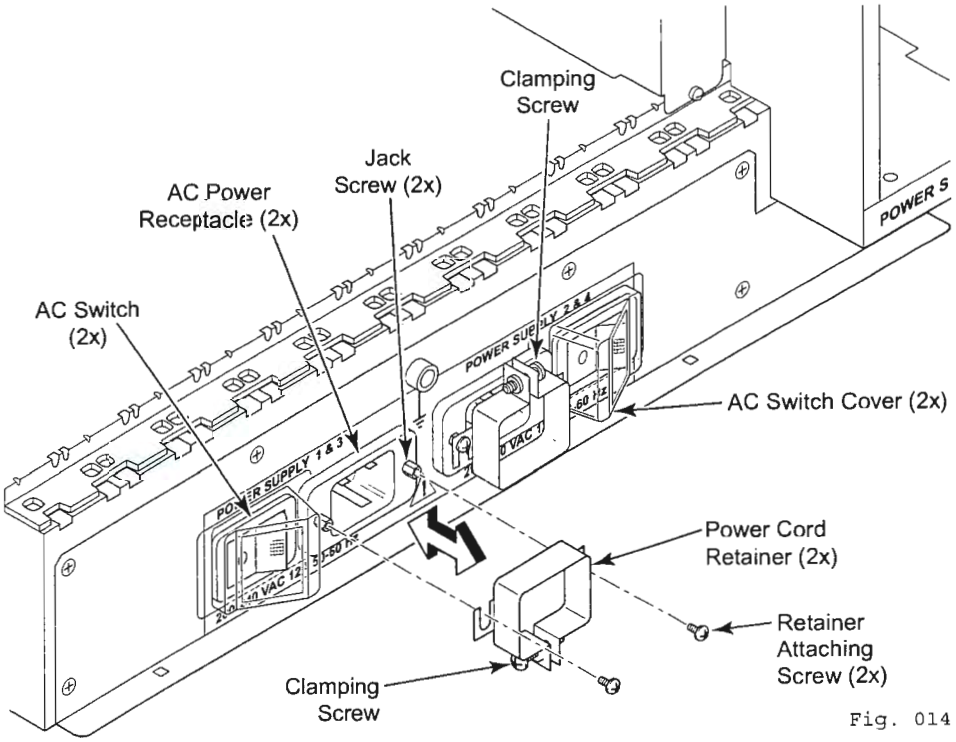


Figure 2-1 AC Panel and Pwer Cord Retainers

Operating Information for the Blower Assemblies

The switch is cooled by three blower assemblies located in the back of the chassis. The air enters through the vents in the blower assembly side of the chassis and exits from the top vent on the port side of the chassis. The chassis requires a minimum airflow of 350 cubic feet per minute.

The blower assemblies are hot-swappable, if two blower assemblies remain operating. If more than one blower assembly must be removed at the same time, turn off the ED-12000B to prevent overheating.

CAUTION

The ED-12000B 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 ED-12000B 16-port cards automatically shut down if the temperature range is exceeded.

CAUTION

Disassembling any part of the blower assembly voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the blower assembly.

Determining the Status of a Blower Assembly

To determine the status of a blower assembly:

1. Check the LED indicators on the blower assembly.
2. Check blower assembly status using the `fanShow` command. The status for each blower assembly displays **OK**, **absent**, or **faulty**. If any of the blower assemblies are faulty, contact EMC technical support. For additional information about the `fanShow` command, refer to the *Fabric OS Reference Manual*.

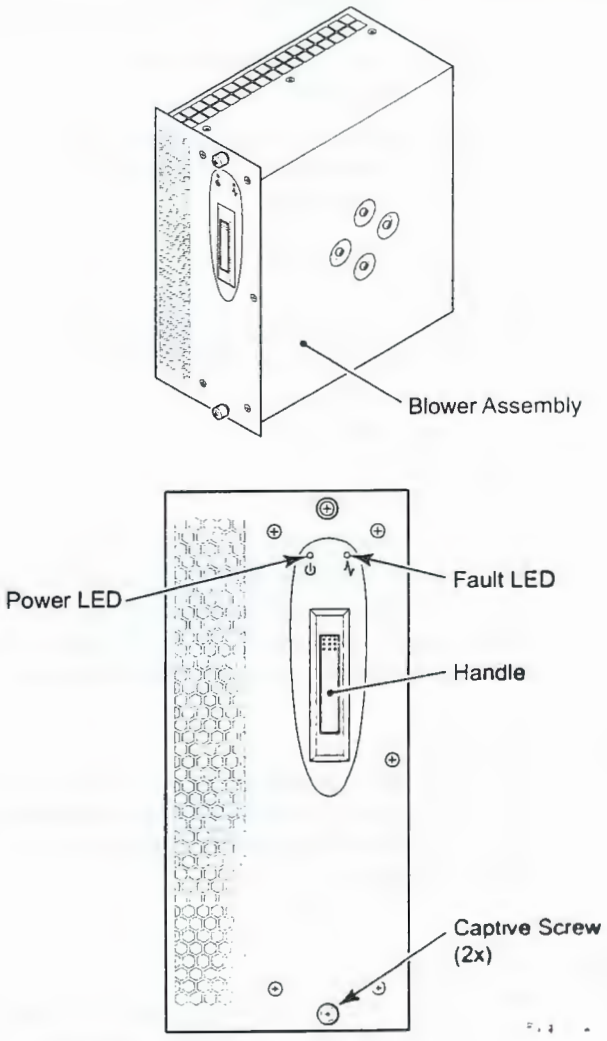


Figure 2-2 Front of a Blower Assembly

Operating Information for the WWN Card and Bezel

The WWN card and bezel are located at the top of the blower assembly side of the chassis.

The WWN card provides LEDs for monitoring the switch from the blower assembly side of the chassis. The WWN card also stores the following information:

- The chassis serial number (used when installing software licenses)
- The two native IP addresses assigned to the CP card slots.
- Information for the two logical switches in the ED-12000B:
  - Switch names
  - IP addresses
  - WWNs
  - Subnet masks

The bezel protects the card and identifies each of the LEDs on the WWN card. Together, the WWN Card and bezel assembly provide 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.

WARNING

Although the information stored in the WWN card is also stored in the flash memory of the CP cards, the switch should not be rebooted while the WWN card is uninstalled; this will cause the switch to boot incorrectly.

CAUTION

Wearing an ESD grounding strap is recommended when working with the WWN card, to prevent damage to the electrical components.

Operating Information for the Chassis

The chassis is highly reliable and unlikely to fail. There are no LEDs specific to the chassis.

Determining the Status of the Chassis

To verify the status of the chassis:

1. Enter the `sensorshow` command to determine component and sensor status.
2. Enter the `slotshow` command to determine slot status.
3. Log into each logical switch and enter the `switchshow` command to determine switch status.

If it appears that a failure may have occurred, refer to *Replacing the Chassis* on page 4-47 for more information on determining whether replacement is necessary.

Managing Cables

The ED-12000B cables can be managed in a variety of ways, including the following:

- Routed down through the cable management tray
- Routed out either side of the chassis
- Cable channels on the sides of the cabinet
- Patch panels

For more information on cable management, refer to *Recommendations for Cable Management* on page 4-15 and *Removing and Installing Cable Management Tray* on page 4-39.

Two items are provided to assist with cable management:

- *Cable Management Tray* — The Cable Management Tray is attached to the bottom of the chassis, and can be used 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 are provided with the ED-12000B, and can be used 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 serve to keep the cables evenly spaced and to hold them away from the 16-port cards to make card replacement easier and to prevent the cables from bending to less than the minimum bend radius.

CAUTION

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 2 inches under full tensile load, and 1.2 inches with no tensile load.

Tie wraps are not recommended for optical cables because they are easily overtightened.

To keep LEDs visible and make it easy to replace components, route cables down in front of the cards, not across adjacent cards or in front of the power supplies. Figure 2-7 on page 2-21 provides an example in which cables for each card are routed in front of that card and are out of the way of other components.

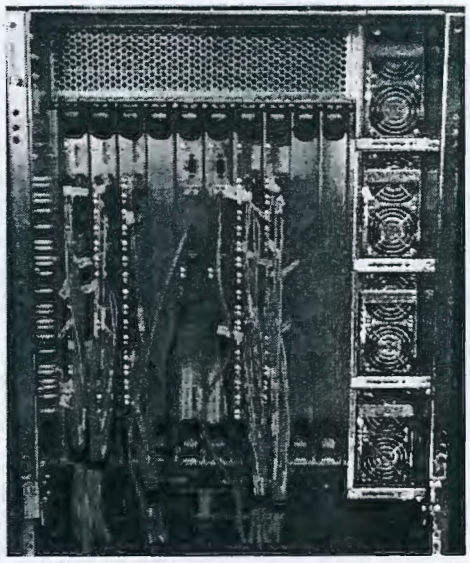


Figure 2-3 Effective Cable Management

Leave at least one meter of slack for each fiber optic cable. This provides room to remove and replace the port card, allows for inadvertent movement of the rack, and helps prevent the cables from being bent to less than the minimum bend radius. Use the cable guides provided with the ED-12000B to group the cables. These guides help to keep individual ports accessible by keeping the cables evenly spaced. If ISL Trunking is in use, grouping the cables by trunking group is recommended.

For information about ISL Trunking, refer to the *ISL Trunking User's Guide.*

Interpreting LED Activity

System activity and status can be determined through the activity of the LED indicators on the switch.

There are three possible LED states:

- No light
- Steady light, in one of the following colors:
  - Green
  - Orange (may be referred to as *amber* in other documentation)
  - Yellow (appears when both green and orange LED elements are lit)
- Flashing light (green, orange, or yellow)

The LEDs may flash green, yellow, or orange while the switch is booting or while POST or other diagnostic tests are running. This is normal, and does not indicate a problem unless the LEDs do not indicate that all components are operational after boot process, POST, and any diagnostic tests are complete.

Any errors are listed in the error log. For information about the error log, refer to *Diagnostic and System Error Message Reference Manual.*

LEDs on the 16-Port Card

The 16-port card has a Power LED and a Status LED (see Figure 2-4). In addition, each of the 16 ports has two LEDs to the left of the port, a Port Status LED and a Port Speed LED.

The LEDs patterns may temporarily change during POST and other diagnostic tests.

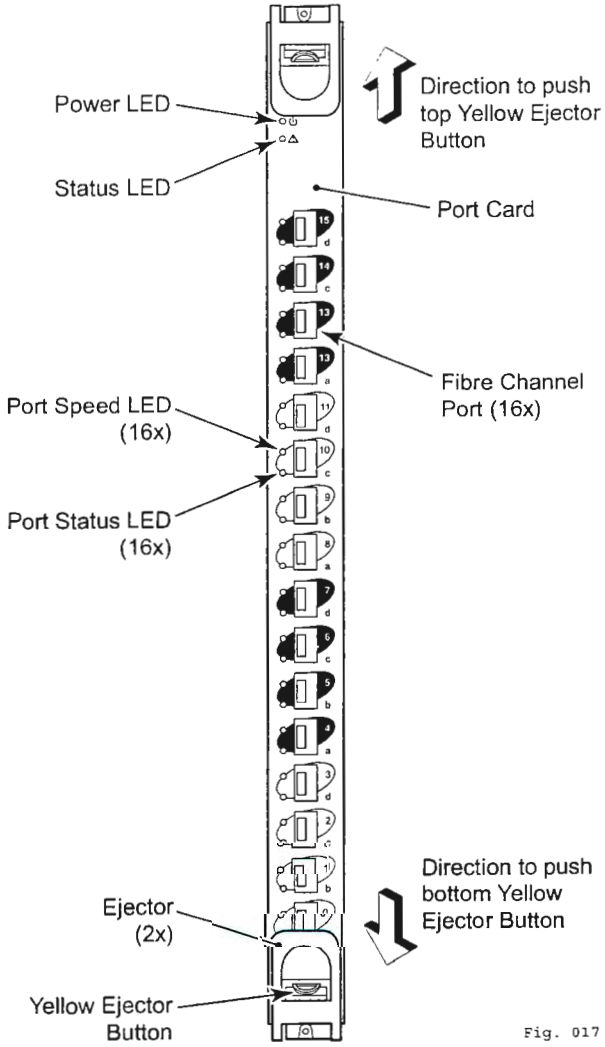


Figure 2-4 Front of 16-Port Card

Table 2-1 16-Port Card LED Patterns

Location of LED on Card	Purpose of LED	Color of LED	Status of Hardware	Recommended Action
Top LED ⏻	Power	No light (LED is off)	16-port card does not have incoming power.	Ensure card is firmly seated and has power.
		Steady green	16-port card has incoming power.	No action required.
Second LED ⚠	Status	No light (LED is off)	16-port card is either healthy or does not have power.	Verify Power LED is lit.
		Steady yellow	16-port card is faulty.	Ensure card is firmly seated, and check status with `slotShow` command. If LED is still yellow, consult switch supplier.
		Slow-flashing yellow (on 2 second; off 2 second)	16-port card is not seated correctly, or is faulty.	If light continues to flash, pull card out and reseat. If LED continues to flash, replace card.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	Environmental range exceeded.	Check for out-of-bounds environmental condition.
Left of each port, upper LED	Port Speed	No light (LED is off)	Port is either set to 1 Gb/s mode, or does not have incoming power.	Verify Power LED is lit. To change the mode, refer to the *Fabric OS Procedures Guide.*
		Steady green	Port is set to 2 Gb/s mode.	No action required.
Left of each port, lower LED	Port Status and Activity	No light (LED is off)	Either the 16-port card does not have incoming power or there is no light or signal carrier detected.	Verify that Power LED is lit, and check transceiver and cable.
		Steady green	Port is online (connected to an external device) but has no traffic.	No action required.
		Slow-flashing green (on 1 second; off 1 second)	Port is online but segmented, indicating a loop back plug or cable, or an incompatible switch.	Verify correct device is connected to port.

Table 2-1 16-Port Card LED Patterns (*continued*)

Location of LED on Card	Purpose of LED	Color of LED	Status of Hardware	Recommended Action
		Fast-flashing green (on 1/4 second; off 1/4 second)	Port is in internal loop back (diagnostic).	No action required.
		Flickering green	Port is online, with traffic flowing through port.	No action required.
		Steady yellow	Port is receiving light or signal carrier, but is not yet online.	No action required.
		Slow-flashing yellow (on 2 seconds; off 2 seconds)	Port is disabled (diagnostic tests or `portDisable` command).	Reset port from workstation.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	Transceiver or port is faulty.	Change transceiver or reset switch from workstation.
		Alternating green and yellow	Port is bypassed.	Reset port from workstation.

LEDs on the Control Processor Card

The CP card has four LEDs: a CP Card Power LED, a CP Card Status LED, a Link Status and Activity LED, and a Link Speed LED (see Figure 2-5).

The LEDs patterns may temporarily change during POST and other diagnostic tests.

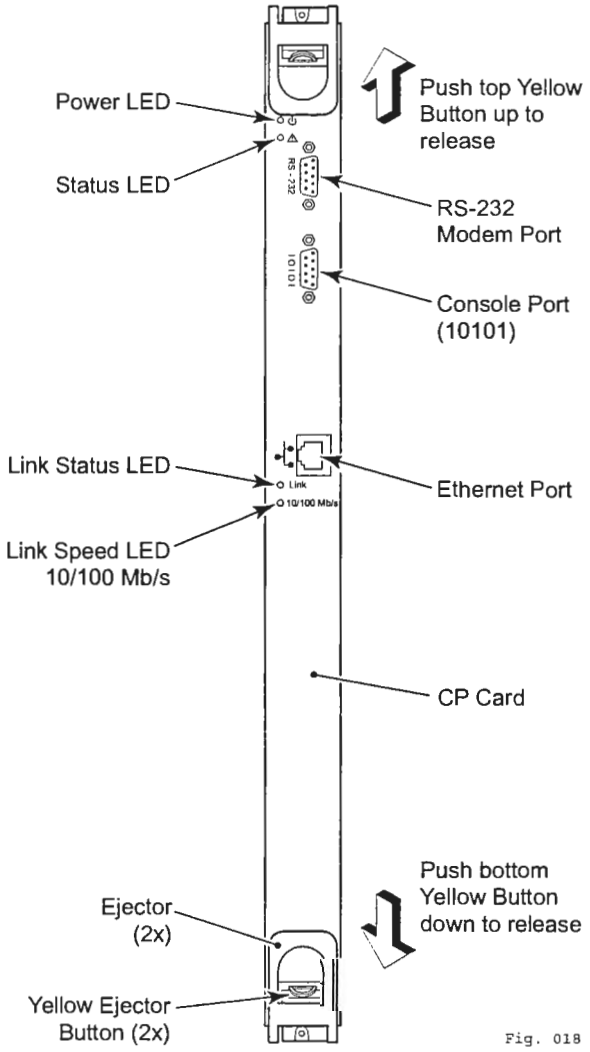


Figure 2-5 Front of Control Processor Card

Table 2-2 Control Processor Card LED Patterns

Location of LED	Purpose of LED	Color of LED	Status of Hardware	Recommended Action
Top LED ⏻	Power	No light (LED is off)	CP card does not have incoming power.	Ensure CP card is firmly seated and has power.
		Steady green	CP card has incoming power.	No action required.
Second LED ⚠	Status	No light (LED is off)	CP card is either healthy or does not have incoming power.	Verify Power LED is lit.
		Steady yellow	CP card is faulty or the switch is still booting.	Ensure CP card is firmly seated. If LED is still yellow, consult switch supplier.
		Slow-flashing yellow (on 2 second; off 2 second)	CP card is not seated correctly or is faulty.	Pull unit out and reseat. If LED continues to flash, replace unit.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	Environmental range exceeded.	Check for out-of-bounds environmental condition.
Link LED	Link Status and Activity	No light (LED is off)	Either CP card does not have incoming power or no link is detected.	Ensure CP card has power, and verify Ethernet cable is firmly seated and device at other end of link is functioning.
		Flickering green and yellow	Link is healthy, with traffic flowing through port.	No action required.
10/100 Mb/s LED	Link Speed	No light (LED is off)	Either link speed is 10 Mb/s or CP card does not have incoming power.	Ensure CP card has power. To force a persistent link speed, enter the ifmodeset command.
		Steady green	Link speed is 100 Mb/s.	No action required

LEDs on the Power Supplies

As shown in Figure 2-6, each power supply has three LEDs: the top LED is the Power Supply Power LED, the center LED is the Power Supply Predictive Failure LED, and the lower LED is the Power Supply Fail LED.

If only one AC power switch is turned on, the Fail LED on each of the two power supplies without power will light up.

The LEDs patterns may temporarily change during POST and other diagnostic tests.

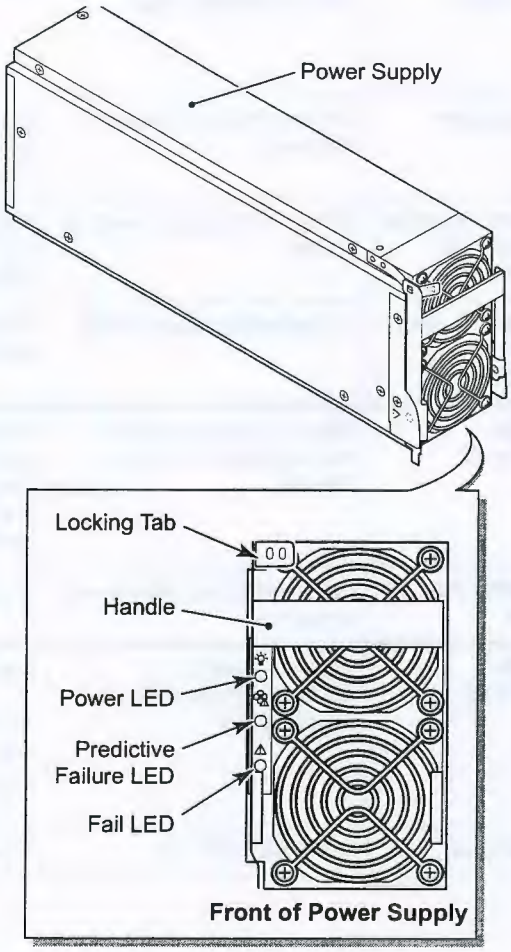


Figure 2-6 Power Supply

Table 2-3 Power Supply LED Patterns

Location of LED	Purpose of LED	Color of LED	Status of Hardware	Recommended Action
Upper LED 	Power	No light (LED is off)	Power supply does not have incoming power and is not providing power to switch.	Ensure power supply is firmly seated, switch has incoming power, both power cables are connected, and AC power switches are on.
		Steady green	Power has incoming power and is providing power to switch.	No action required.
Center LED 	Predictive Failure	No light (LED is off)	Power supply is either healthy or does not have incoming power.	Check Power LED.
		Flashing orange (amber)	Power supply is about to fail due to a failing fan inside the power supply.	Replace power supply.
Lower LED 	Fail	No light (LED is off)	Power supply is either healthy or does not have incoming power.	Check Power LED.
		Steady orange (amber)	Either the switch has power but this power supply does not (AC switch may be off), or the power supply has failed.	Ensure correct AC power switch is on and power supply is seated. If orange light continues, replace power supply.
		Flashing orange (amber)	Power supply is unable to supply power.	Verify incoming power meets requirements listed in *Power Specifications* on page A-5.

LEDs on the Blower Assemblies

Each blower assembly has two LED indicators: a Power LED and a Fault LED (see Figure 2-7).

The LEDs patterns may temporarily change during POST and other diagnostic tests.

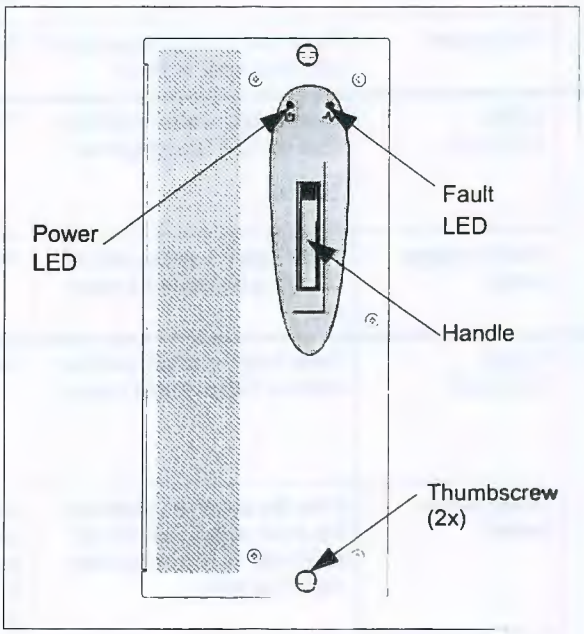


Figure 2-7 Blower Assembly

Table 2-4 Blower Assembly LED Patterns

Location of LED	Purpose of LED	Color of LED	Status of Hardware	Recommended Action
Left LED ⏻	Power	No light (LED is off)	Blower assembly does not have incoming power.	Ensure blower assembly is firmly seated and has power.
		Steady green	Blower assembly has incoming power.	No action required.
Right LED ⎍	Fault	No light (LED is off)	Blower assembly is either healthy or does not have incoming power.	Ensure blower assembly has incoming power.
		Steady orange	Blower assembly has fully or partly failed.	Replace blower assembly.
		Slow-flashing orange (on 2 second; off 2 second)	Blower assembly is not seated correctly or is faulty.	Pull unit out and reseat. If LED continues to flash, replace unit.
		Fast-flashing orange (on 1/2 second; off 1/2 second)	Environmental range exceeded.	Check for out-of-bounds environmental condition.

Determining the Status of the WWN Card

Check the LEDs on the WWN card and verify that they reflect the actual status of the components. The WWN card is highly reliable and unlikely to fail. If it appears that a failure may have occurred, refer to *Replacing the WWN Card* on page 4-45 for more information on determining whether replacement is necessary.

LEDs on the WWN Card and Bezel

The WWN card and bezel are located at the top of the blower assembly side of the chassis. The bezel covers the card, allowing the LEDs to shine through (see Figure 2-8 on page 2-26). The card and bezel provide 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, CP card, or 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 WWN card flashes, the Power LED on the WWN card also flashes for increased visibility. The LED patterns may temporarily change during POST and other diagnostic tests.

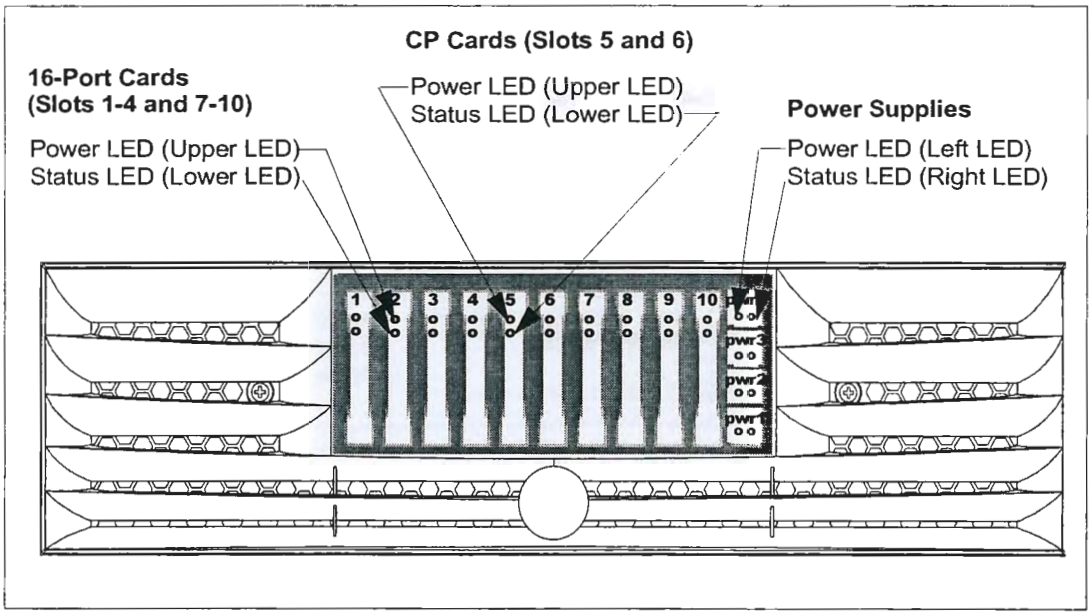


Figure 2-8 WWN Card and Bezel

Interpreting POST Results

Each time the switch is powered on or reset, the switch automatically performs POST, a system check during which LED patterns may vary.

To verify that POST has completed without errors:

- Verify that all LEDs return to a normal state after 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 *Effective Cable Management* on page 2-14. Use the `slotShow` command to check status of the slots.

  For information about setting a switch to beacon, refer to the *Fabric OS Procedures Manual*.

- Verify that the switch prompt displays when POST completes.

  If it does not display, POST was not successfully completed. Contact EMC for support.

- Review the system log.

  Any errors detected during POST are written to the system log, which is accessible through the `errShow` command. For information about error messages, refer to the *Diagnostic and System Error Message Reference Manual*.

3 Configuring the ED-12000B Switch

This chapter contains the following topics:

Configuring the ED-12000B

Overview

The ED-12000B can contain up to two logical switches, each with its own configuration: one logical switch for any 16-port cards in slots 1-4, and 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. It is automatically mirrored to the standby CP card, so that the most current configuration remains available even if the active CP card fails. In addition, the configuration can be backed up by uploading the configuration to a workstation using the `ConfigUpload` command, and can be downloaded to the active CP card using the `ConfigDownload` command. For information about commands and whether they can be entered through the active or standby CP card, refer to the *Fabric OS Reference Manual*.

A routine backup of the configuration is recommended, to ensure the current configuration is available if needed.

The configuration can be modified only through a login session to the active CP card. The ED-12000B 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 is automatically changed on switch 1.

The ED-12000B configuration includes the following parameters:

- General system parameters (modifiable through the `configure` command): For information about modifying these parameters through the `configure` command, refer to the *Fabric OS Reference Manual*.
- WWNs for both logical switches: The two WWNs are not modifiable; both are pre-configured and are usually based on the chassis serial number.
- Domain ID: The default domain ID for switch 0 is 1; switch 1 has a default ID of 2.
- One domain ID for any 16-port cards in slots 1-4, and one for any 16-port cards in slots 7-10 (domain IDs can be modified through the `configure` command).

- Native IP addresses: A native IP address, host name, subnet mask, and gateway address for both CP card slots (modifiable through the `ipAddrSet` command).
- Logical IP addresses: A logical IP address and subnet mask for both logical switches (modifiable through the `ipAddrSet` command).

Resetting a logical IP address while the switch has active IP traffic such as Web Tools, Fabric Watch, SNMP, and other applications, may cause them to be interrupted or stopped.

Items Required

The following items are required to configure and connect the ED-12000B:

- ED-12000B powered on but not connected to a network or fabric
- Workstation computer with a terminal emulator application (such as HyperTerminal)
- Serial cable provided with the switch
- Ethernet cable
- Small form factor pluggable (SFP) transceivers and cables, as required
- Two IP addresses for use as the *native* IP addresses assigned to the CP slots, with the corresponding native host names, subnet masks, 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 use as the *logical* IP addresses of the switch, with the corresponding subnet masks. 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
- 10.77.77.76 sw1

◆ Two switch names, if the default switch names are not going to be used.

Switch names can be up to 15 characters long, can include alpha, numeric, and underscore characters, and must begin with an alpha character. The default switch name for the logical switches are sw0 for the switch containing the 16-port cards in slots 1-4, and sw1 for the switch containing 16-port cards in slots 7-10.

Configuration Procedure

1. Verify that the ED-12000B is on and POST is complete by verifying that all power LED indicators on the 16-port cards and CP cards are displaying a steady green light.

   For a description of the LED patterns, see Chapter 2, *Starting and Operating the ED-12000B Switch*.

2. Log on to the CP card installed in slot 5 by establishing a serial connection to a workstation that has a terminal emulator application (such as HyperTerminal on Windows 95, Windows 2000 or Windows NT, or TERM in a UNIX environment).

   a. Disable any serial communication programs 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 (see Figure 2-5 on page 2-20).

   c. Connect the other end of the serial cable to a serial port on the workstation.

      If necessary, the adapter on the serial cable can be removed to allow for an RJ45 serial connection.

   d. Open the terminal emulator application and configure as described below.

      – For Windows 95, Windows 98, Windows 2000, or Windows NT, enter the following parameters:

Parameter	Value
Bits per second:	9600
Databits:	8
Parity:	None
Stop bits:	1
Flow control:	None

- For most UNIX systems, enter the following string at the prompt:

```
tip /dev/ttyb -9600
```

e. When the terminal emulator application stops reporting information, press ENTER to get the following login prompt:

```
CP0 Console Login:
```

f. Enter the administrative logon information.

The default administrative logon is `admin`.

g. Enter `0` at the following prompt to log in to switch 0:

```
Enter switch number to login <0 or 1>: 0
```

At the initial login the user is prompted to enter new Admin and User passwords. The same administrative account applies to both logical switches. If the password is changed on switch 0, it is automatically changed on switch 1.

h. Modify passwords if desired. Passwords must be a total of 8 to 40 characters long, and should include a combination of numbers and upper case and lower case letters.

To skip modifying the password, press CTRL-C.

3. Determine which CP card is active by entering the following command:

```
haShow
```

This command provides the following information:

```
switch:admin> haShow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby
HA Enabled, Heartbeat Up
```

For greater detail, refer to the *Fabric OS Reference Manual*.

4. Configure the IP addresses for both CP cards.

Configuration changes can only be made through a session with the active CP card, although you can assign IP addresses to either CP card from a 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 log on as **admin**.

b. Enter the `ipAddrSet` command at the prompt, enter `2` for the CP card in slot 5, and `3` for the active CP card in slot 6. For example:

```
ipAddrSet 2
```

c. Enter the requested information at the prompts, as shown below (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 [switch0]:
Gateway Address [0.0.0.0]:
```

The host name is the native name assigned to the CP card. The same gateway address must be used 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 reboot.

d. Repeat Step 4a through Step 4c for the other CP card.

5. Configure the two logical IP addresses.

Resetting a logical IP address while the switch has active IP traffic such as Web Tools, Fabric Watch, SNMP, and other applications, may cause them to be interrupted or stopped.

a. To configure the first logical IP address, enter the following command at the prompt:

```
ipAddrSet 0
```

b. Enter the requested information for this IP address at the prompts:

```
Ethernet IP Address [10.77.77.77]:
Ethernet Subnetmask [0.0.0.0]:
Fibre Channel IP Address [none]:
Fibre Channel Subnet Mask [none]:
```

The Ethernet IP address and the Fibre Channel IP address must be on different networks.

The logical IP address is updated immediately.

c. To configure the second logical IP address, enter the following command at the prompt:

ipAddrSet 1

d. Enter the requested information for this IP address at the prompts, as described in Step 5b.

e. Reboot the CP card by entering the following command at the prompt:

switchreboot

The terminal serial port can be used to monitor error messages through a serial connection. EMC does not recommend using it as a command interface during normal operations because it only modifies one switch at a time (switch 0 by default).

f. If this port is not going to be in on-going use, remove the serial cable and protect the port from dust by replacing the shipping cap.

6. Optional: Connect the Ethernet hub in the cabinet to a 10/100 Mb local area network (LAN).

   a. Insert one end of an ethernet cable into one of the empty ports in the cabinet's ethernet hub.

   b. Connect the other end to an ethernet 10/100 Base-T LAN.

The switch can now be accessed by remote connection using any of the available management tools, such as Telnet or Web Tools. Ensure that the switch is not modified from other connections during the rest of this procedure.

7. Optional: Log on to either of the logical switches by Telnet, using the administrative logon.

The default administrative logon name is `admin`.

The switch can now be accessed remotely, using Telnet or Web Tools. Ensure that the switch is not being modified from any other connections during the remaining steps. The ED-12000B supports up to two Telnet sessions with administrative privileges at the same time.
The remaining steps in this procedure can be accomplished through 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.

Changing the switch name causes a domain address format RSCN to be issued.

---

   a. Enter the command `switchName` with the new name in quotes as follows (`sw10` is an example name):

      `switchName "sw10"`

      For more information about the `switchName` command, refer to the *Fabric OS Reference Manual*.

   b. Record the new switch name for future reference.

   c. To customize the switch name for the other logical switch, logout of the CP session, connect the serial cable to the other CP card, log in as **`admin`**, and then repeat Step 8a and Step 8b for the other logical switch.

9. Optional: Specify any custom status policies.

   a. To access the status policy, enter the following command at the prompt:

      `switchStatusPolicySet`

   b. Complete the prompts to specify the desired policies.
      To completely deactivate the alarm for a particular condition, enter `0` at the prompt for that condition.

10. Check the ED-12000B for switch and port status by entering the following command at the Telnet prompt:

    `switchShow`

This command provides detailed information about the switch. For more information about this command, refer to the *Fabric OS Reference Manual*.

11. Check the fabric for ISLs, switch names, or other status by entering the following command at the Telnet prompt:

    `fabricShow`

    This command provides general information about the fabric. For more information about this command, refer to the *Fabric OS Reference Manual*.

12. After all zoning configurations and other changes are complete, back up the configuration by entering 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. For more information about this command, refer to the *Fabric OS Reference Manual*.

A routine backup of the configuration is recommended.

4

Maintaining the ED-12000B Switch

This chapter provides the following information:

Overview

The ED-12000B does not require any regular physical maintenance, and is designed to minimize the chance of failure.

The power supplies, 16-port cards, CP cards, and blower assemblies can all be replaced in the field without special tools. The ED-12000B can continue operating during the FRU replacements if the conditions specified in the corresponding procedures are followed.

If a Fabric Watch license is installed on the ED-12000B, Fabric Watch alarms can be configured for each FRU. For more information, refer to the *Fabric Watch User Guide*.

To determine the status of individual FRU hardware and whether or not the hardware is functioning correctly, visually check the LEDs for the hardware components (refer to *Effective Cable Management* on page 2-14), or use the commands described in *Environmental Status and Maintenance Commands* on page 4-4.

Performing Diagnostic Tests

Diagnostic tests are provided to help troubleshoot the hardware and the firmware. The diagnostic tests provided on the switch include tests of internal connections and circuitry, and SFPs and fiber optic cables in use. The tests are implemented by command, either through a Telnet session or through a terminal set up for a serial connection to the switch. Some tests require the ports to be connected to each other by external cables, to allow diagnostics to verify the serializer/deserializer interface and to test the attached SFP and cable.

All diagnostic tests are run at link speeds of 1 Gb/s and 2 Gb/s. For information about diagnostic tests and how to run them, refer to the *Diagnostic and System Error Message Reference Manual*.

Diagnostic tests may temporarily lock the transmit and receive speed of the links to a specific speed.

Environmental Status and Maintenance Commands

The following commands display environmental and other information. For additional information about these commands, refer to the *Fabric OS Reference Manual*.

The environmental commands report internal temperatures within the chassis. The port cards can withstand internal temperatures of up to 75 degrees Celsius, and the CP cards can continue to operate up to 80 degrees celsius. However, the ambient temperature outside the chassis must be 40 degrees Celsius or less.

Commands are shown here with mixed capitalization for easier reading, but can be entered with all lower-case characters.

Table 4-1 Environmental Status and Maintenance Commands

Command	Information Displayed
`chassisshow`	Displays serial number, time awake, and other information about each operating component
`slotshow`	Whether each slot is occupied and the status of that card is in the slot.
`sensorshow`	◆ Temperature readings for the port cards in the logical switch currently logged into ◆ Temperature readings for the CP cards ◆ Status and RPM of all operational fans ◆ Status of all operational power supplies
`psshow`	Status of all operational power supplies
`fanshow`	Status and RPM of all operational fans
`errshow`	Switch error log, which lists the status of any marginal/failed components
`tempshow`	◆ Temperature readings for the port cards in the logical switch currently logged into ◆ Temperature readings for the CP cards

chassisShow This command provides information about all the FRU components.

Example (truncated):

```
switch12k:admin> chassisShow
   SW BLADE  Slot: 3
   Header Version:          1
   Power Consume Factor:    -180
   Brocade Part Num:        60-0001532-03
   Brocade Serial Num:      1013456800
   Manufacture:           Day: 12  Month:  6  Year: 2001
   Update:                Day: 15  Month:  7  Year: 2001
   Time Alive:              28 days
   Time Awake:              16 days
   ID:                      555-374757
   Part Num:                234-294-12345
   Serial Num:              2734658
   Revision Num:            A.00

   CP BLADE  Slot: 6
   Header Version:          1
   Power Consume Factor:    -40
   Brocade Part Num:        60-0001604-02
   Brocade Serial Num:      FP00X600128
   Manufacture:           Day: 12  Month:  6  Year: 2001
   Update:                Day: 15  Month:  7  Year: 2001
   Time Alive:              61 days
   Time Awake:              16 days
   ID:                      555-374757
   Part Num:                236-296-12350
   Serial Num:              2836542
   Revision Num:            A.00

   <output truncated>
```

slotShow This command displays info about which slots are occupied and the status of that card is in the slot.

Example:

```
switch:admin> slotShow
   Slot    Blade Type    ID     Status
   ---------------------------------
   1       SW BLADE      2      FAULTY
   2       SW BLADE      2      DISABLED
   3       SW BLADE      2      ENABLED
   4       SW BLADE      2      DIAG RUNNING POST2
   5       CP BLADE      1      ENABLED
   6       CP BLADE      1      ENABLED
   7       UNKNOWN              VACANT
   8       SW BLADE      2      DIAG RUNNING POST1
   9       SW BLADE      2      INSERTED, NOT POWERED ON
   10      UNKNOWN              VACANT
```

sensorShow This command displays the current temperature readings, fan status and RPM, power supply and fan readings from sensors. This command is per logical switch.

Example:

```
sw0_155:admin> sensorShow
sensor  1: (Temperature) is Ok, value is 36 C
sensor  2: (Temperature) is Ok, value is 35 C
sensor  3: (Temperature) is Absent
sensor  4: (Temperature) is Absent
sensor  5: (Temperature) is Ok, value is 21 C
sensor  6: (Temperature) is Ok, value is 21 C
sensor  7: (Fan         ) is Ok, speed is 2576 RPM
sensor  8: (Fan         ) is Ok, speed is 2481 RPM
sensor  9: (Fan         ) is Ok, speed is 2463 RPM
sensor 10: (Power Supply ) is Ok
sensor 11: (Power Supply ) is Faulty
sensor 12: (Power Supply ) is Ok
sensor 13: (Power Supply ) is Faulty
```

psShow This command displays the current status of the power supplies.

Example:

```
sw0_155:admin> psShow
Power Supply #1 is OK
Power Supply #2 is OK
Power Supply #3 is OK
Power Supply #4 is OK
```

fanShow This command displays status and RPM of the blower assemblies.

Example:

```
sw0_155:admin> fanshow
Fan #1 is OK, speed is 2576 RPM
Fan #2 is OK, speed is 2481 RPM
Fan #3 is OK, speed is 2481 RPM
```

errShow Displays the switch error log, which lists the status of marginal/failed components. The following example shows that the Switch 0 blower assembly has failed.

Example:

```
sw0_155:admin> errshow
Error 15
--------
0x2e3 (fabos): Dec 29 15:57:34
Switch: 0, Error FW-BELOW1, 3, envFan001 (Env Fan 1) is
   below low boundary. current value : 0 RPM. (faulty)
```

tempshow Displays current temperature readings for the CP cards and all the port cards belonging to the current logical switch.

Example:

```
switch:admin> tempshow

switch:admin> tempshow
Index Slot   State  CentigradeFahrenheit
=============================================================
   =
1     5      Ok     27          80
2     6      Ok     27          80
3     7      Ok     44          111
4     8      Absent
5     9      Ok     40          104
6     10     Absent

switch:admin>
```

Removing and Installing a 16-Port Card or Filler Panel

This procedure provides instructions for removing a ED-12000B 16-port card or filler panel, then installing either a 16-port card or filler panel. The ED-12000B can continue to operate during this procedure. However, if a 16-port card is being removed, any cables connected to that 16-port card must be disconnected.

You can notify the ED-12000B of a hot swap request in two ways: the commands `slotPowerOff` and `slotPowerOn`, or by clicking the ejector handles on the 16-port card.

CAUTION

Do not uninstall the 16-port card during diagnostic tests. Wait for the Status LED to turn off in response to the hot-swap request before uninstalling a 16-port card.

Port cards can be installed 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.

For information about how to check the status of hardware components using command line interface, refer to the *Fabric OS Procedures Manual*.

CAUTION

Disassembling any part of a 16-port card or filler panel voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the 16-port card or filler panel. To ensure correct cooling of the chassis and protection from dust, install a filler panel in any empty slots.

Time Required 10 minutes or less.

Procedure

CAUTION

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).

To remove a port card (see Figure 4-1):

1. Ensure traffic is not flowing through the port card (port LEDs should be off) prior to disconnecting cables.

   a. Remove any SFP transceivers and cables from the 16-port card.

   b. Notify the switch of a hot swap request by pushing the yellow tab on each ejector in and clicking the black handles slightly open, and wait for the Status LED to turn off.

   You can also send hot swap notification from the command line interface using the commands `slotpoweroff` and `slotpoweron`. Refer to the *Fabric OS Procedures Guide* for additional command line instructions.

   CAUTION

   If removing a 16-port card, wait for the Status LED (see Figure 2-4 on page 2-17) to turn off in response to the hot swap request before removing the card.

   c. Lever both ejectors open to approximately 45 degrees, and pull the port card out of the chassis.

   If you inadvertently re-latch the ejectors prior to the card being removed, wait at least one second prior to unlatching the ejectors again.

2. If the card is not being replaced by another port card, install a filler panel to ensure correct cooling of the chassis and protection from dust. Refer to *To install a port card for filler panel:* on page 4-13.

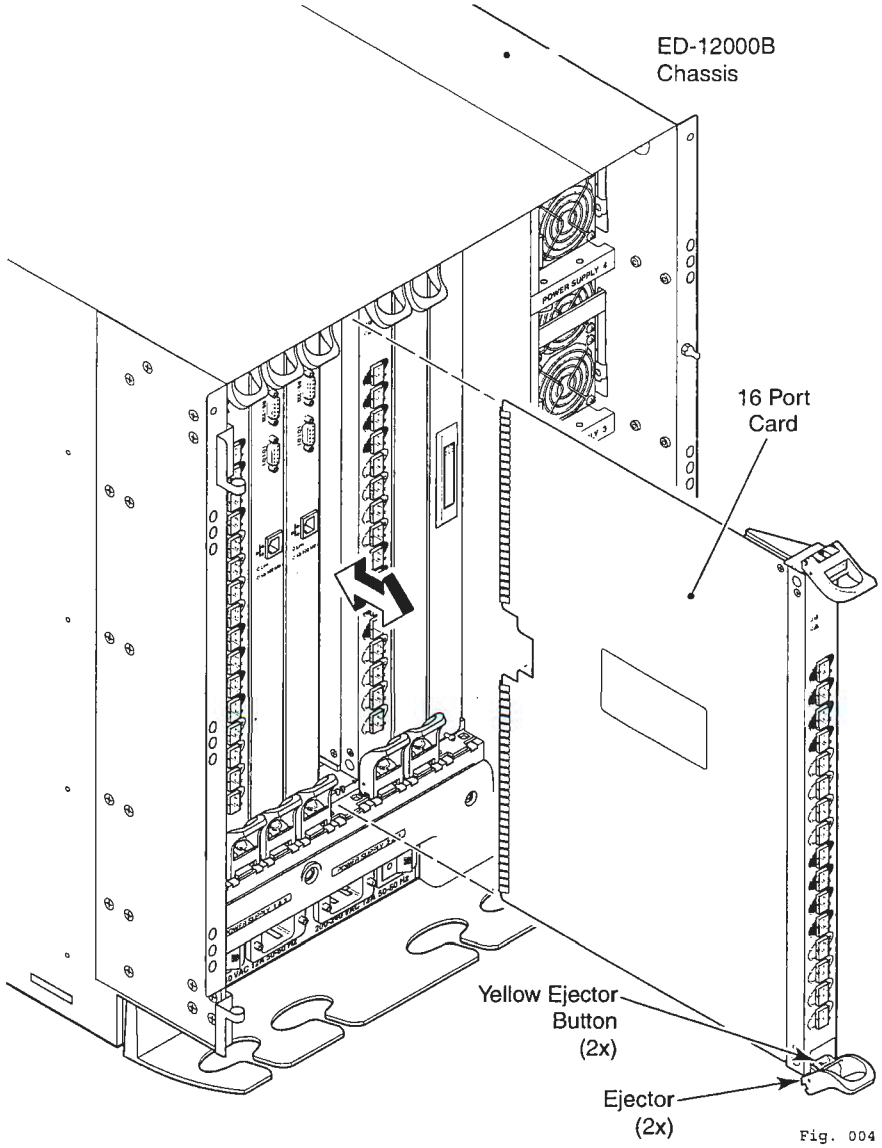


Figure 4-1 Port Card Removal and Replacement

To remove a filler panel:

The ED-12000B accommodates two types of filler panels: one with ejectors, one without (see Figure 4-2 on page -12).

To remove a filler panel with ejectors, follow these steps:

1. Push the yellow tab in on each ejector (see Figure 4-2 on page -12).
2. Lever both ejectors all the way open.
3. Slide the filler panel out of the chassis.

Filler panels without ejectors are equipped with a handle. Remove the two captive screws, grasp the handle, and slide the filler panel out.

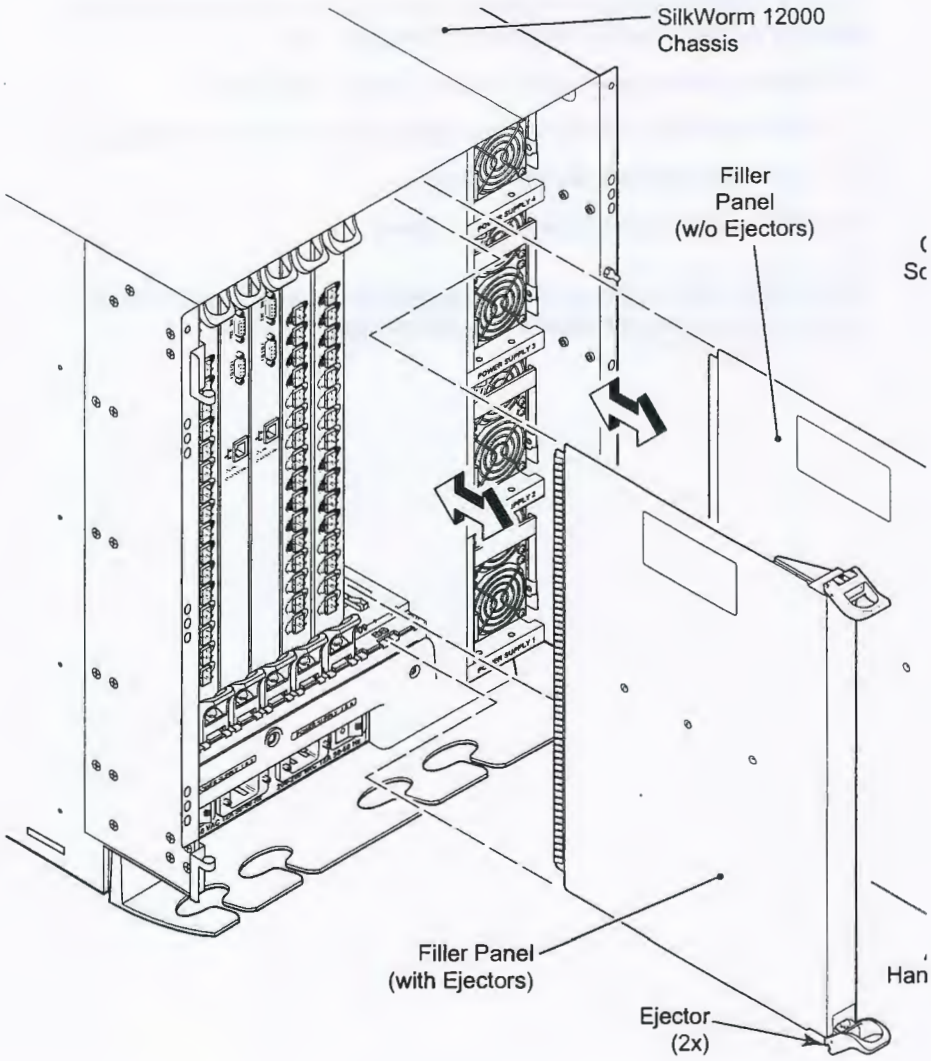


Figure 4-2 Port Card Filler Panel

To install a port card for filler panel:

CAUTION

Do not force the installation. If the 16-port card or filler panel does not slide in easily, ensure it is correctly aligned inside rail guides before continuing. Installing a port card or filler panel with incorrect alignment damages both the chassis and the replacement part. Disassembling any part of a port card or filler panel voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the 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 and lower rail guides in the slot (see Figure 4-3), and 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 (slight audible click). The levering action of the handles seats the 16-port card or filler panel in the slot.

To install a filler panel that does not have ejectors, align the flat side of the filler panel inside the upper and lower rail guides in the slot (see Figure 3-3 on page 3-12), then slide the filler panel into the slot (with slight pressure to the left) until it is firmly seated and tighten the two captive screws.

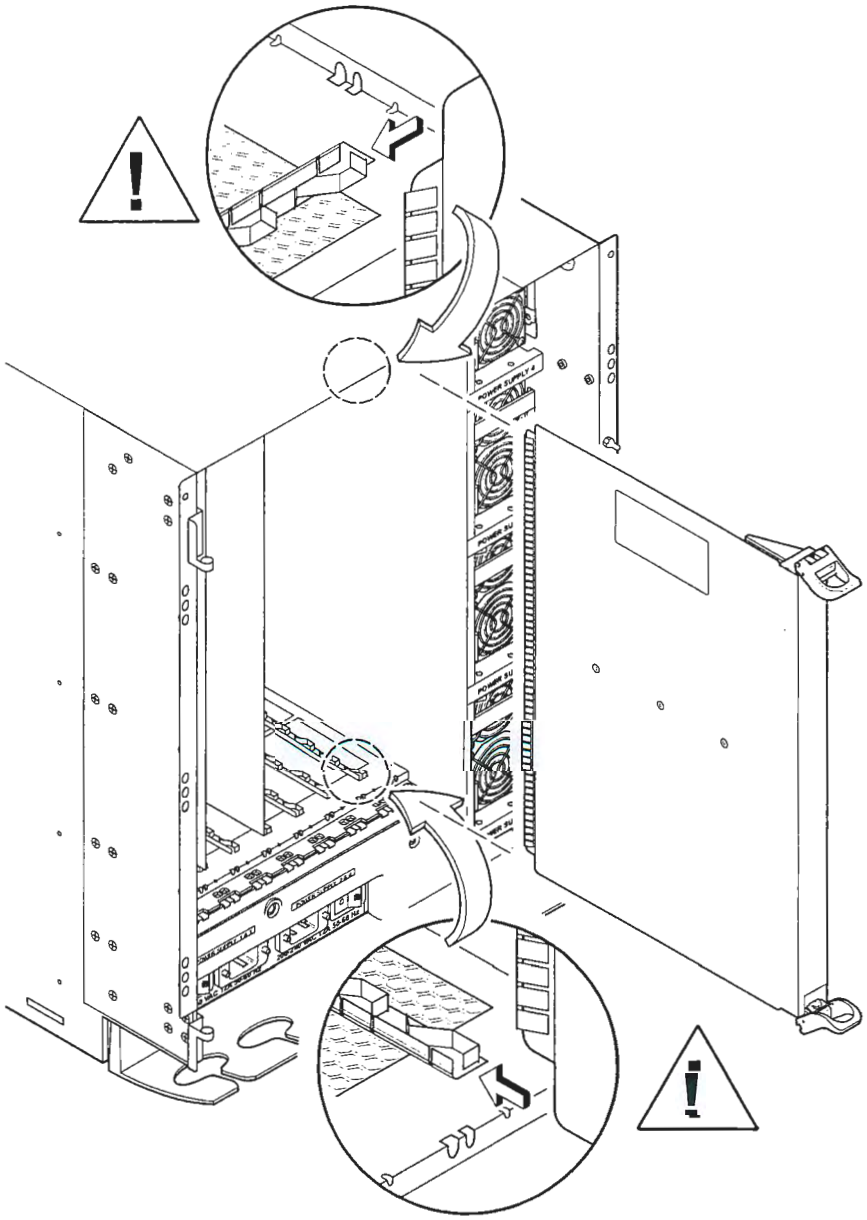


Fig. 028

Figure 4-3 Alignment Guides in Card Slots

Additional steps to complete if a new 16-port card was installed:

1. Verify that the Power LED on the 16-port card is displaying a steady green light (it may require a few seconds to turn on). If it does not turn on, ensure the 16-port card has power and is firmly seated. The front of the 16-port card should be flush with adjacent 16-port cards or filler panels.

   The LED patterns may temporarily change during POST and other diagnostic tests.

2. Install SFP transceivers and cables in the 16-port card, as required.
3. Group and route the cables as desired (cable management recommendations provided in following section).

CAUTION

Do not route cables in front of the exhaust vent (located at the top of the port side of the chassis.

4. Verify the installation. For information about how to check the status of hardware components using command line interface, refer to the *Fabric OS Procedures Guide*.

Recommendations for Cable Management

- Cables can be managed in a variety of ways, such as routed down through the cable management tray or routed out either side of the chassis, and by using patch panels or cable channels on the sides of the cabinet.
- To keep LEDs visible and prevent having to disconnect cables when removing neighboring cards, route fiber optic and other cables directly downwards, instead of across adjacent cards or in front of the power supplies.
- Leave at least one meter of slack for each fiber optic cable. This provides room to remove and replace the 16-port card, allows for inadvertent movement of the rack, and helps prevent the cables from being bent to less than the minimum bend radius (the minimum bend radius for a 50 micron cable is 2 inches under full tensile load and 1.2 inches with no tensile load).

- Use the cable guides provided with the ED-12000B 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, and also help to provide clearance for the removal of a neighboring card.

Removing, and Installing a Control Processor Card

This section provides instructions for replacing, removing and installing a ED-12000B Control Processor card (CP card) or filler panel.

CAUTION

When replacing main chassis components, existing software configurations should be saved.

The ED-12000B 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 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 one minute and occurs automatically as soon as the active CP card is uninstalled.

CAUTION

An active Control Processor card must be installed and functioning properly before attempting to replace a standby Control Processor card. Do not power off system when replacing the Control Processor.

The Telnet command haShow provides information about which CP card is the active CP card. For information about this command, refer to the *Fabric OS Reference Manual*.

The new CP card automatically assumes the IP address and host name assigned to the slot.

For information about how to check the status of hardware components using command line interface, refer to the *Fabric OS Procedures Manual*.

CAUTION

Disassembling any part of a CP card or filler panel voids the part warranty and regulatory certifications. There are no user-serviceable parts 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.

WARNING

Do not attempt to replace the real time clock (RTC) battery on the CP card. There is danger of explosion if the battery is incorrectly replaced. Contact EMC, since the battery must be replaced with the same type of battery as recommended by the manufacturer, and must be disposed of according to the manufacturer's instructions.

Replacing a CP Card

Both logical switches in the ED-12000B can continue to operate while a CP card is replaced if the other CP card continues to operate and no failover occurs (you can prevent failover by entering the `hadisable` command). The active CP card is determined by the most recent failover.

If you need to replace the active CP card and are at an earlier version of Fabric OS (prior to v4.1), traffic through the ED-12000B may be temporarily suspended until failover to the standby CP card is complete.

The configuration on the active CP card is automatically mirrored to the standby CP card; this section includes steps to ensure that the new CP card boots up as the standby CP card.

If the new CP card does not have the same firmware as the active CP card, it must be upgraded/downgraded to the same firmware version.

WARNING

Use the same version of Fabric OS on both CP cards and logical switches. Using different versions may cause malfunctioning. If the replacement CP card has a different version of Fabric OS, bring both cards to the same firmware version.

Time Required

If a firmware upgrade is required, this will take approximately one hour. If no firmware upgrade is required, this will take approximately 30 minutes.

Items Required

- ESD (electrostatic discharge) grounding strap
- Workstation computer
- Serial cable provided with the ED-12000B
- IP address of an FTP server for backing up the switch configuration

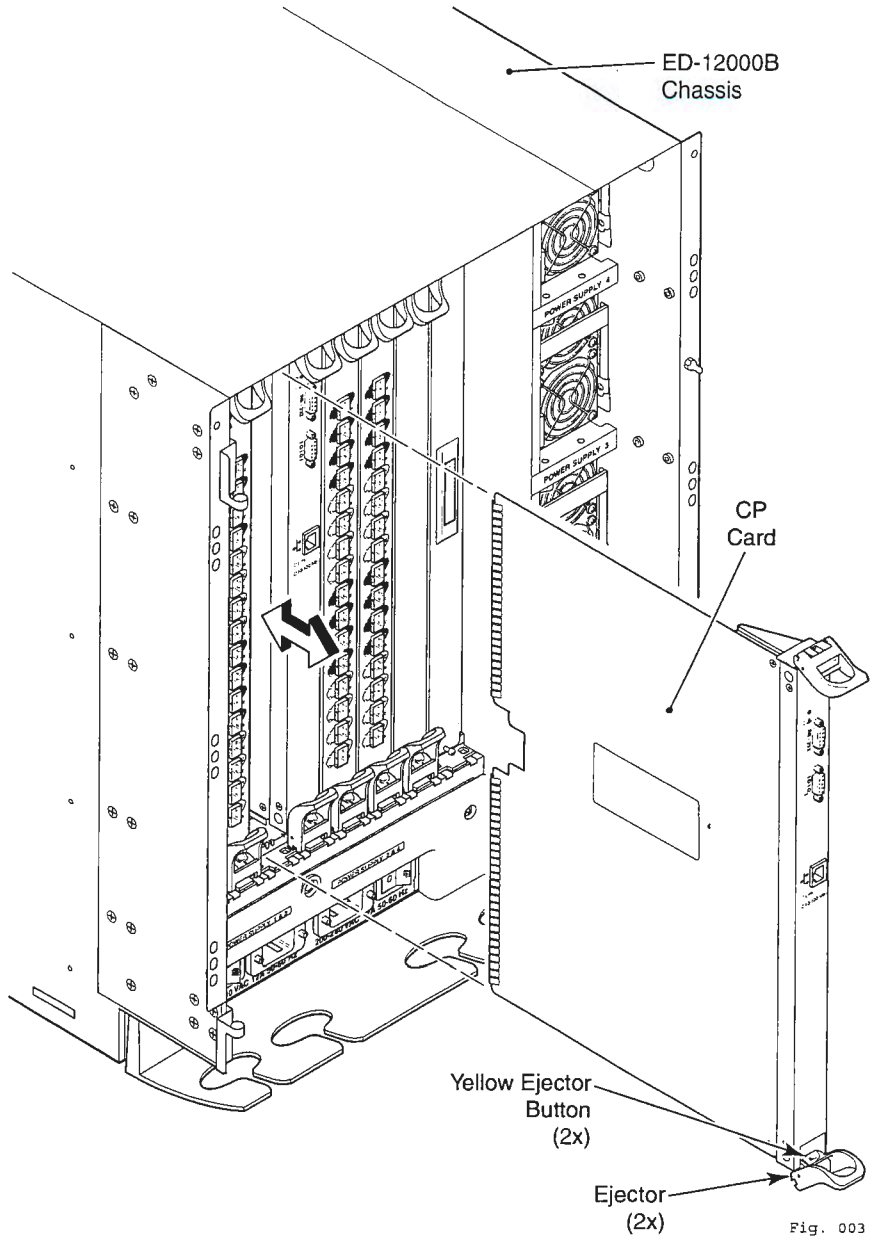


Figure 4-4 CP Card Removal and Replacement

Confirming a Failed CP Card

If you have not already done so, confirm the necessity of replacing the CP card before continuing. The following events may indicate that a CP card is faulty:

- The Status LED on the CP card is yellow, 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 telnet commands or the serial console is not available.
- The `hashow` command indicates that the CP cards have not achieved redundancy (after 30 minutes).
- The calendar clock is inaccurate, or the CP card does not boot up or shut down normally.
- Any of the following messages display in the error log:
  - "Slot unknown" message relating to a CP slot
  - CP card errors or I2C time-outs
  - 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 complete information about diagnostic and error messages, refer to the *Diagnostics and System Error Message Reference*.

If none of the above items are true, and you have not already confirmed the CP card failure with your switch supplier, contact your switch supplier before continuing.

Recording Critical Switch Information

The switch configuration should be backed up before you replace a CP card.

To record critical switch information:

1. Create a serial connection to the healthy CP card:

a. Disable any serial communication programs running on the workstation (such as synchronization programs).

b. Connect a serial cable to the console port. Refer to Figure 2-2 on page -11.

c. Connect other end of serial cable to a serial port on the workstation.

If necessary, the adapter on the serial cable can be removed to allow for a serial RJ45 connection.

---

d. Open the terminal emulator application and configure as follows:

For Windows 95, 98, 2000, or NT	Parameter	Value
	Bits per second	9600
	Databits	8
	Parity	None
	Stop bits	1
	Flow control	None

For most UNIX systems, enter the following string at the prompt:

```
tip /dev/ttyb -9600
```

e. When the terminal emulator application stops reporting information, press Enter.

2. Log into the healthy CP card as Admin, then enter "0" to log into Switch 0 (see below example).

Example Sample output for logging into switch 0 from a serial console

```
Fabric OS (cp0)
cp0 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin>
```

3. Enter the `hashow` command to determine which CP card is active.

Example Sample output for the `hashow` command:

```
SW0:admin> haShow
Local CP (Slot 5, CP0) : Active
Remote CP (Slot 6, CP1) : Standby, Healthy
HA Enabled, Heartbeat Up
SW0:admin>
```

Enter all remaining commands from the serial console for the *active* CP card, unless otherwise indicated. For more information about commands, refer to the *Fabric OS Reference Manual*.

4. If the healthy CP card is performing as the active CP card, continue with Step 7 on Page 4-24. If the faulty CP card is performing as the active CP card, fail over the cards as described below sample.

   a. Create a serial connection to the faulty CP card Step 1 on Page 4-21.

   b. Log into the serial console as admin and enter "0" to log into logical Switch 0.

   c. Enter 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 (indicates failover is complete).

   e. Enter the `hashow` command from the serial console for the healthy CP card to verify the failover.

Example Sample of logging into Switch 0 from a serial console, then failing over:

```
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. Enter the `version` command to record the version of the active CP card.
6. Enter 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 sample of backing up the configuration for logical switch 0 and switch 1, in step 8):
   a. Enter the `configupload` command.

   The `configupload` command uploads the switch configuration to a specified FTP server.

   ---

   b. Enter the requested information at the prompts.
8. Log into logical Switch 1 and back up the current configuration for Switch 1 (see example below):
   a. From the serial console for the healthy CP card, enter the `login` command.
   b. Log in as admin and enter "1" to log into Switch 1.
   c. Enter the `configupload` command.
   d. Enter the requested information at the prompts.

Example Sample of backing up the configuration for logical switch 0 and switch 1:

```
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

To remove a CP card:

CAUTION

Wear a grounded ESD strap when handling a CP card. A grounding connection is available on the chassis above the power connectors (see Figure 4-4 on page 4-20). Hold CP cards by the edges of the metal pans, not by the ejector handles. To allow the current configuration to be copied to the new CP card, a new CP card must be installed while the other CP card is still operating.

1. Disconnect all cables:
   - Modem cable from modem serial port
   - Serial cable from terminal serial port
   - Ethernet cable from ethernet port
2. Notify the switch of a hot swap request by pushing the yellow button on each ejector all the way in and clicking the black handles slightly open. Wait for the Power LED to turn off

CAUTION

Do not remove the CP card until the Power LED has turned off.

3. Lever both ejector handles open to approximately 45 degrees and pull the CP card out of the chassis

CAUTION

Do not force the ejector handles open. If they do not open easily, verify that the yellow buttons are pressed all the way in.

Installing a CP Card

To install a new CP card in the slot:

CAUTION

DO NOT FORCE THE INSTALLATION. If the CP card does not slide in easily, ensure it is correctly oriented and aligned in the card guides before continuing (see Figure 4-3 on page -14).

1. Open the ejector handles to approximately 45 degrees, then orient the CP card so that the handles are towards you, and the flat metal side is on the left.
2. Align the flat metal side of the CP card inside the lower and upper card guides in the slot as shown in Figure 4-3 on page -14, then slide the CP card into the slot until it is firmly seated.
3. Close the ejectors by pressing the black handles in toward the CP card until they click.
4. Verify that the Power LED is green (may require a few seconds). If not, ensure the CP card has power, is firmly seated, and the ejectors are in the locked position.
5. Connect the modem, serial, and ethernet cables as required to the new CP card.

CAUTION

Do not route cables in front of the exhaust vent (located at the top on the port side of the chassis).

Verifying Operation of the New CP Card

To verify operation of the new CP card:

1. Verify that boot and POST are complete on the new CP card (a minimum of 3 minutes), and 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 on the active CP card displays yellow until the active CP card is fully operational, and the Status LED on the standby CP card displays yellow until the CP cards have achieved failover redundancy.

b. From the serial console for the active CP card (should still be the CP card that was not replaced), enter the `hashow` command, and verify that the command output includes "HA Enabled Heartbeat Up" and "HA-state in sync."

If not, POST is not complete or the CP cards have not yet achieved redundancy (as shown in the sample below). Wait a minute or two and re-enter the command, until you can verify that redundancy has been achieved.

Example Sample output for 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>
```

If `hashow` command indicates any errors after redundancy is achieved, contact the switch supplier.

2. Enter the `slotshow` command. The command output should show the new CP card as "enabled" (see below sample).

Example Sample output for the `slotshow` command:

```
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 version (see sample below):
   - For any firmware version, you can enter the `version` command.
   - For Fabric OS v4.0.0d and later firmware, the `firmwareshow` command is available.

Example Sample output for the `version` and `firmwareshow` commands:

```
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 does not match the active CP card, bring the replacement card to the same firmware level as the active card. Check the EMC Support Matrix for supported versions.
   a. Download the firmware, using either of the following command options (see sample output for the firmwaredownload command, below):
      - Enter **`firmwaredownload`** 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, a message displays warning you that this command causes the active CP card to reset. If this message displays, enter "**y**" to continue.
      - Telnet into the CP that you want to download firmware to. Enter the `firmwaredownload -s` command to download the firmware to only one of the CP cards. Enter all requested information and choose the *reboot* option.

   For more information about the `firmwaredownload` command, refer to the *Fabric OS Reference*.

Example 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 #############################################
<some output not shown>
glibc ################################################
sin ##################################################
Write kernel image into flash.
file verification SUCCEEDED
Firmwaredownload completes successfully.
SW1:admin>
```

5. Verify the reboot is complete and the CP cards have achieved failover redundancy.
   a. Wait until the Status LEDs on both CP cards are not lit.
   b. Enter the `hashow` command, and verify that the command output includes "HA Enabled Heartbeat Up". If not, wait a minute and reenter the command, until you have verified that redundancy is achieved.
6. Enter the `version` or `firmwareshow` command to verify the firmware version has been updated (see sample output of the version and firmwareshow command in step 3).
7. Create a serial connection to the new CP card (instructions provided in Step 1 on Page 4-21).
8. Log into the new CP card as Admin, entering "0" to log into logical Switch 0 (see sample below).

Example Sample output for logging into switch 0 from a serial consol:

```
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, enter 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, enter the `configshow` command followed by a text string (in quotes) that relates to the parameter. For example, `configshow "fabric"`. This limits the command output to entries that contain that text string (see sample below).

Entering the `configshow` command *without* a filter prints out approximately 1000 lines. For more information about this command refer to the *Fabric OS Reference Manual*.

Example Sample output for the `configshow` command with the "fabric" as 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
<remaining output not shown>
SW0:admin>
```

11. If the switch configuration does not appear to have replicated correctly, download the switch configurations that were backed up earlier (refer to Step 7 and Step 8 on Page 4-24). Refer to the sample of the output for downloading the switch configurations below.
    a. Enter the `switchdisable` command to disable the current logical switch (should still be Switch 1).
    b. Enter the `configdownload` command and enter the requested information.

If the switch is running Fabric OS v4.0.2, a message displays cautioning you about downloading the correct configuration file. If this message displays, enter "**y**" to continue.

c. Once the configuration has been downloaded, enter the `switchenable` command.

d. Log into Switch 0, then repeat Step a - Step c above.

Example Sample output for downloading configuration to both logical switches:

```
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
cp1 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>
```

About 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, then the battery may need to be replaced. Contact EMC if the RTC begins to lose time.

WARNING

Do not attempt to replace the real time clock (RTC) battery on the CP card. There is danger of explosion if the battery is incorrectly replaced. Contact EMC, since the battery must be replaced with the same type of battery as recommended by the manufacturer, and must be disposed of according to the manufacturer's instructions.

Removing and Installing a Power Supply

Use this procedure to remove and install a power supply. The ED-12000B can continue operating during the replacement if at least one power supply continues operating for every four 16-port cards installed. EMC requires a minimum of four power supplies.

You do not need to notify the ED-12000B of a hot swap request before removing a power supply.

The left power connector provides power to the power supplies in slots #1 and #3, and 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 4-5 on page 4-35 for power supply location.

For information about how to check the status of hardware components using command line interface, refer to the *Fabric OS Procedures References Manual*.

CAUTION

To protect against AC failure, EMC recommends a minimum of one power supply in slot #1 or slot #3, and one in slot #2 or #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.

Disassembling any part of the power supply voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the power supply.

Time Required Less than 5 minutes.

Procedure

1. Determine whether adequate power to keep the chassis operating will be available throughout the replacement.
   If adequate power will NOT be consistently available, shut down the switches gracefully as follows:
   a. Open a telnet session to the active CP card and log into Switch 1 as Admin.
   b. Enter the `switchshutdown` command.

c. After the message "`Cleaning up kernel modules.....Done`" displays, repeat Step a through Step c for Switch 0.

d. Power off the chassis: Flip both AC power switches to the off position (the "0" on the switch).

2. If the ED-12000B is going to continue operating during the replacement procedure, check the LEDs to verify that the minimum of two power supplies are functioning before uninstalling the power supply being replaced.

3. Remove the current power supply or filler panel from the chassis. See Figure 4-5 on page 4-35.

CAUTION

Support the power supply from underneath while removing it from the chassis.

a. To remove a power supply, push 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.

4. Install the new power supply or filler panel.

CAUTION

Do not force the installation of the power supply. If the part does not install easily, ensure it is properly oriented.

a. To install a power supply, orient it so the handle is toward the front of the chassis and the LEDs are on the left, unlock the handle, then insert the power supply all the way into the slot and push the handle up until it clicks.

b. Verify the power supply is seated by pulling gently on the handle.

5. If a power supply was installed, verify the top LED on the power supply displays a steady green light. If it does not, ensure both power cables are plugged in and both AC switches are flipped to `1` (AC switch lights up green).

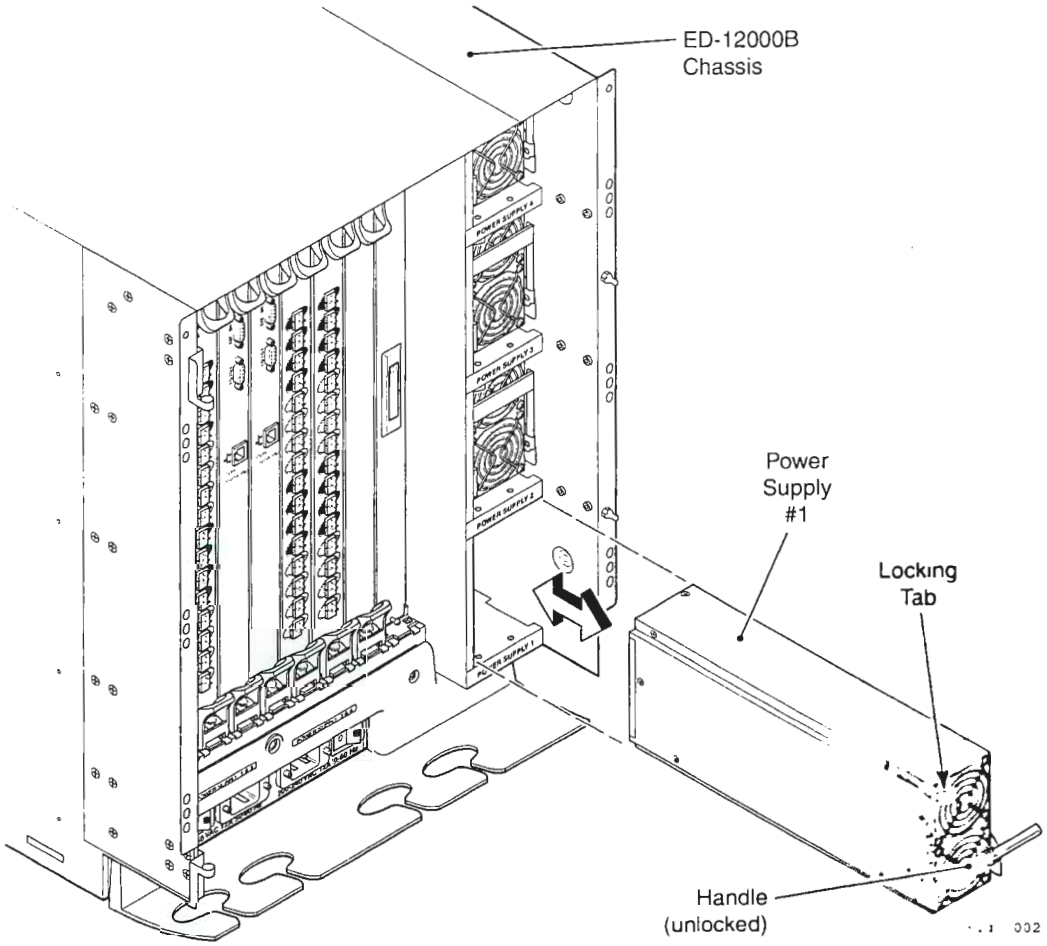


Figure 4-5 **Power Supply Removal and Replacement**

Removing and Installing a Blower Assembly

This procedure provides instructions for removing and installing the blower assembly for the ED-12000B. The ED-12000B requires a minimum of two operating blower assemblies, and can continue operating 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, the ED-12000B should be turned off to prevent overheating.

You do not need to notify the ED-12000B of a hot swap request before removing a blower assembly.

WARNING

The ED-12000B 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

CAUTION

Disassembling any part of the blower assembly voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the blower assembly.

Time required: Less than 5 minutes.

Items required: #2 straight screwdriver

Procedure

1. Before removing the blower assembly, verify 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 4-6 on page 4-38 for LED locations).

   For information about how to check the status of hardware components using command line interface, refer to the *Fabric OS Procedures Manual*.

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.

b. Push in the top of the handle, then pull out the lower part and pull the blower out of the chassis.

3. Install the new blower assembly in the chassis.

CAUTION

Do not force the installation. If the blower assembly does not slide in easily, ensure it is properly oriented before continuing with the installation.

a. Orient the blower assembly as shown in Figure 4-6 and slide into the chassis, pushing firmly to ensure it is seated.

b. Verify that the Power LED displays a green light. If not, ensure that the blower assembly is seated correctly.

c. Push the top of the handle into the recess.

d. Tighten the thumbscrews to finger-tight.

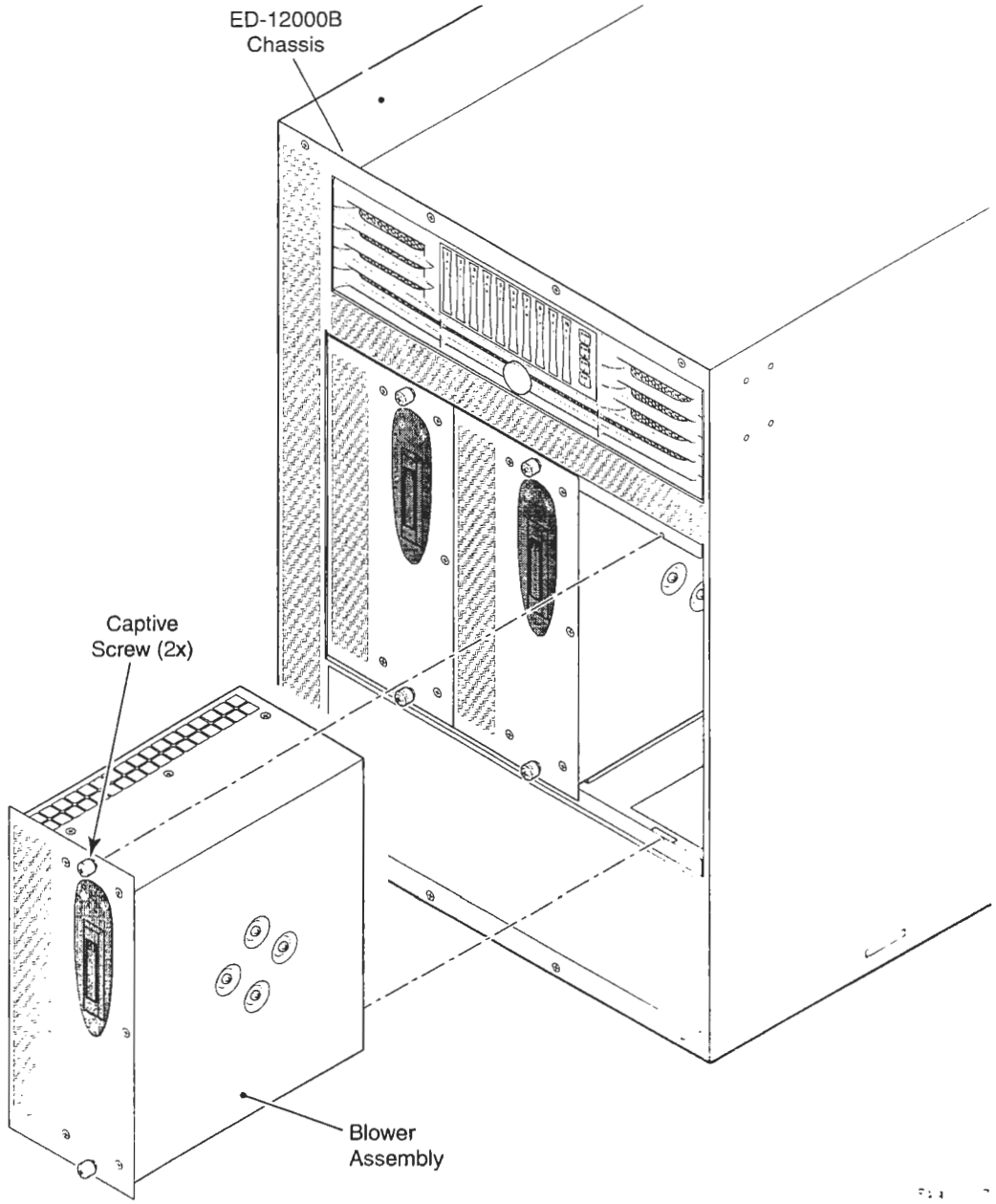


Figure 4-6 Blower Assembly Side of ED-12000B (shown with one blower assembly uninstalled)

Removing and Installing Cable Management Tray

This procedure provides instructions for removing and installing the cable management tray for the ED-12000B. The ED-12000B can continue to operate during the installation.

CAUTION

Do not use a power screwdriver on the cable management tray.

Time Required Less than 5 minutes.

Items Required #2 Phillips screwdriver

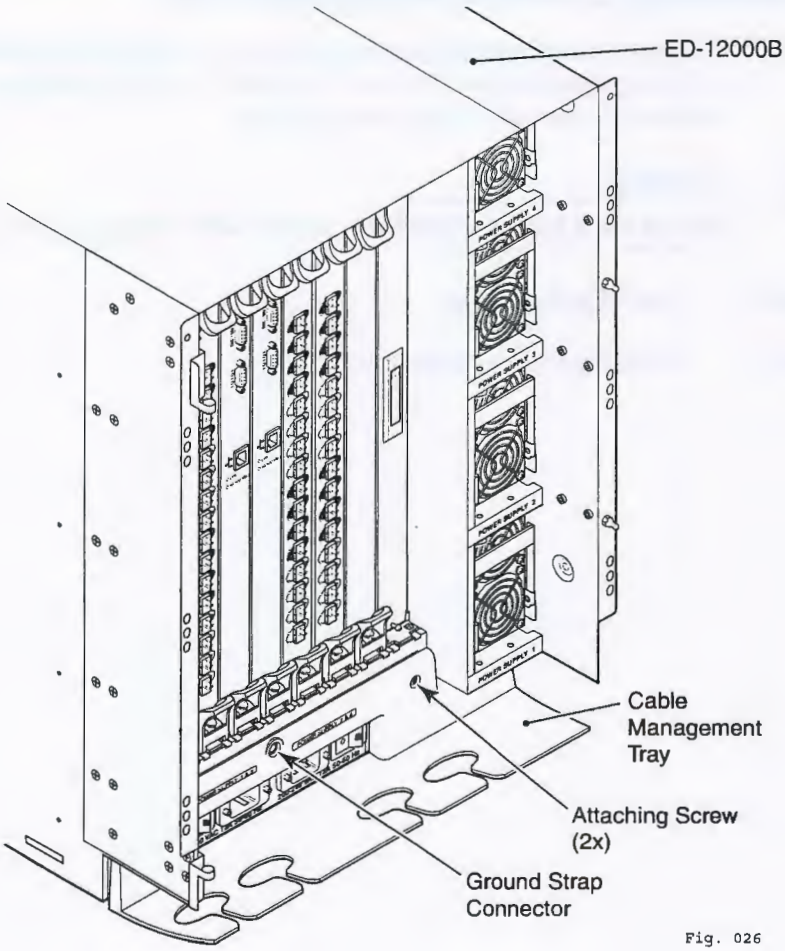


Figure 4-7 Cable Management Tray

Procedure

1. Uninstall the current cable management tray, if still installed (see Figure 4-7 on page 4-40).
   a. Pull any cables out of the tray.
   b. Unscrew the two screws holding the tray to the chassis (see Figure 4-7 for location of screws) and save for reuse.

c. Rotate the front of the tray down, then lift the back to disengage the tabs on the back from the chassis.

2. Install the new cable management tray.

   a. Orient tray as shown in Figure 4-7 on page 4-40 and insert the two tabs on underside of tray into the two slots at the bottom of the AC panel, then rotate front of tray upward until it locks into place.

   b. Position and tighten the two screws saved from Step 1b.

   c. Arrange the cables through or along the tray as required.

EMC recommends routing the power cables out each side of the chassis.

Replacing the Cable Management Guides

The cable guides can be used 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 also serve to keep the cables evenly spaced and hold them away from the port card to prevent the cables from bending to less than the minimum bend radius.

CAUTION

Do not route the cables in front of the air exhaust vent (located at the top of the front of the chassis).

The minimum bend radius for a 50-micron cable is 2 inches under full tensile load, and 1.2 inches with no tensile load.

Tie wraps are not recommended for optical cables, because they are easily overtightened.

To use the cable management guides, orient the guides horizontally and insert the cables into the holes, using a separate hole for each cable.

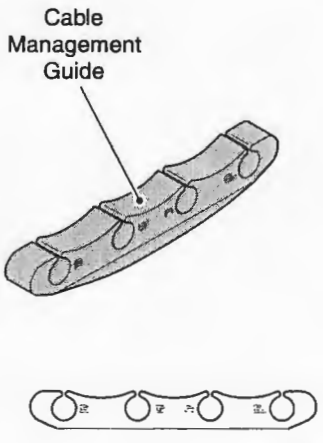


Figure 4-8 Cable Management Guide

Replacing the Chassis Door

The chassis door is available if you have a stand-alone unit.

This procedure provides instructions for replacing the chassis door on the ED-12000B.

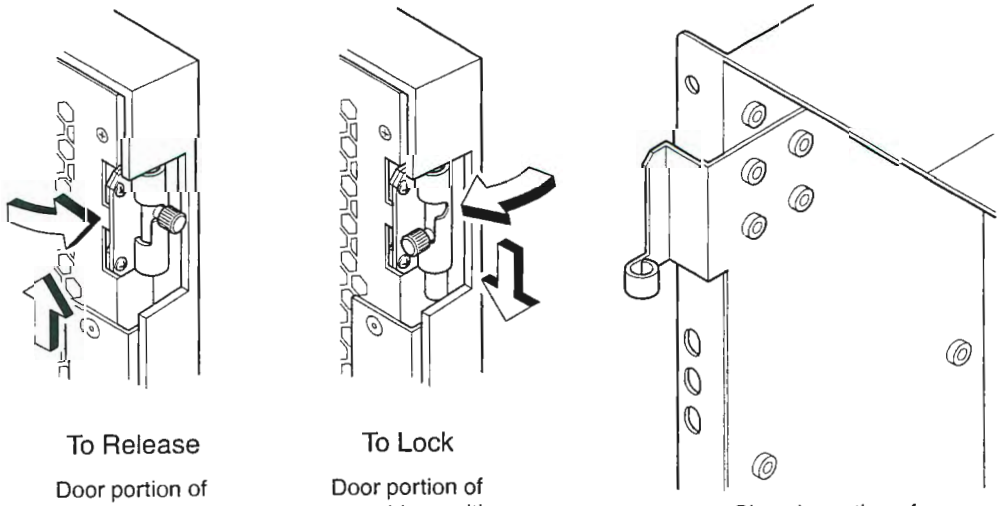
The chassis door is required to ensure the ED-12000B meets EMI and other regulatory certifications.

Time Required Less than 5 minutes

Items Required Chassis door

Procedure

1. Remove the current door from the chassis. See Figure 4-9 for the following steps.
   a. Open the door to a 90 degree angle.
   b. Push the lever on the spring-loaded pin on the upper hinge up and into the notch in the hinge.
   c. Push the lever on the spring-loaded pin on the lower hinge down and into the notch in the hinge, supporting the door to prevent it from falling.



To Release

Door portion of upper hinge with pin in notch

To Lock

Door portion of upper hinge with pin out of notch (Pin released)

Chassis portion of upper hinge

Fig. 011

Figure 4-9 Door and Chassis Portion of Upper Door Hinge

2. Install the new door in the chassis.
   a. Ensure that the levers on the spring-loaded pins on both hinges are pushed into the notches.
   b. Align the spring-loaded pins with the chassis portion of the hinges.
   c. Release the pins by pushing the levers out of the notches.

Replacing the WWN Card

The WWN card is highly reliable. Before replacing the WWN card, verify the replacement is necessary.

Instructions are provided with the replacement chassis.

For versions of Fabric OS prior to v4.1, replacing the WWN card requires power cycling the ED-12000B.

CAUTION

If the WWN card does fail, do not remove it until the replacement card has been received.

Follow the instructions provided with the new WWN card.

Do not reboot the switch with a failed or missing WWN card.

Verifying Necessity of Replacement

Ensure the current card is firmly seated when performing troubleshooting steps, and contact your support provider if you have any questions about whether the card should be replaced.

Any of the following events may indicate that the card requires replacement:

- Visible mechanical damage to the WWN card
- Any of the Status LEDs on the WWN card do not reflect the actual status of the components
- Problems viewing or modifying the data stored on the WWN card (see *Data Stored on the WWN Card*, below)
- Error messages regarding WWN units #1 or #2 (see *Messages That May Indicate WWN Card Failure*, below)

Data Stored on the WWN Card

The following data is stored on the WWN card. Difficulty retrieving or modifying this data may indicate WWN card failure.

Table 4-2 Data Stored on the WWN Card

Data	Related Commands
WWN values	wwn, chassisshow
License keys	licenseshow, licenseadd, licenseremove
Data about the chassis and WWN card	chassisshow
Ethernet and fibre channel IP address information for the CP (control processor) cards	ipaddrshow, ipaddrset
History log information	historyshow, historylastshow
Names of logical switches	switchname

Messages That May Indicate WWN Card Failure

If the error log or serial console display error messages indicating problems with WWN units #1 or #2, the WWN card may have failed. WWN units #1 and #2 correspond to information specific to the WWN card, and are displayed by the `chassisshow` command.

WWN units #1 and #2 do not correspond to the WWNs for logical switches 0 and 1.

For more information about error messages, refer to the *Diagnostics and System Error Message Reference.*

Table 4-3 Messages That May Indicate WWN Card Failure

Type of Message	Sample Error Message
WWN unit #1 or #2 fails its FRU (field replaceable unit) header access	0x24c (fabos): Switch: 0, error EM-I2C_TIMEOUT, 2, WWN 1 I2C timed out: state 0x4
WWN unit #1 or #2 is being faulted	0x24c (fabos): Switch: 0, Critical EM-WWN_UNKNOWN, 1, Unknown WWN #2 is being faulted
WWN unit #1 or #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

Replacing the Chassis

The ED-12000B chassis is highly reliable. Before replacing the chassis, verify the replacement is necessary.

Instructions are provided with the replacement chassis.

Replacing the chassis requires powering off the ED-12000B, disconnecting all cables, and gaining root access to the ED-12000B.

CAUTION

Disassembling any part of the chassis voids the part warranty and regulatory certifications. There are no user-serviceable parts inside the chassis.

Follow the backup instructions provided with the new chassis.

Verifying Necessity of Replacement

Before replacing the chassis, verify the replacement is necessary. Ensure the components are firmly seated when troubleshooting, and contact your support provider if you have any questions about whether the chassis should be replaced.

Any of the following events may indicate that the chassis requires replacement:

- Visible mechanical damage to the chassis, including damage to sheet metal or card guides that prevents correct installation of a component
- Bent or damaged connectors on the main backplane (the surface inside the chassis to which CP cards and port cards connect) or on the blower backplane (the surface to which the blower assemblies connect)
- One or more ED-12000B components (such as a power supply, blower assembly, port card, CP card, or WWN card) do not function properly even after the component is replaced
- An AC power switch shuts off automatically even though all power supplies are removed from the chassis
- The `psshow` or `fanshow` commands continue to show a faulty component even though the component has been replaced
- The `slotshow` command continues to show a faulty CP card or port card even though the card has been replaced

Replacing the 14U Rack Kit

The 14U Rack Kit can be used to install the ED-12000B in a 19-inch wide EIA (Electronics Industry Association) rack. It is compatible with both round and square-holed rails.

Instructions are provided with the kit.

A

Product Specifications for the ED-12000B

This appendix provides the following information:

ED-12000B Components

The ED-12000B consists of the following components:

- A 14U chassis, designed to be mounted in the Connectrix EC-1230B cabinet.
- A minimum of 4 port cards, compatible with SFPs (small form factor pluggable media)
- 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 10/100 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 that flows from the blower side of the chassis to the port side of the chassis. The fans provide adequate cooling for the maximum switch power rating of 102 Watts.

Physical Dimensions

The dimensions of the ED-12000B are listed in the following table.

Table A-1 Physical Specifications

Dimension	Value
Height	<14U (24.11 inches; 61.2 cm)
Depth	27.9 inches (70.9 cm)
Depth with Door	28.7 inches (72.9 cm)
Width	17.2 inches (43.7 cm)

ED-12000B and Component Weights

The weight of a fully loaded ED-12000B, as well as the weights of individual components, are listed in the following table.

Table A-2 Component Weights

Component	Value
Fully Loaded Chassis	Approx. 250.0 pounds (114 kg)
Empty Chassis	104.0 pounds (47.1 kg)
Door	7.6 pounds (3.4 kg)
Blower Assembly	8.8 pounds (4 kg)
Power Supply	7.0 pounds (3.2 kg)
WWN Bezel	0.6 pounds (0.27 kg)
CP Card	5.6 pounds (2.5 kg)
16-Port Card	8.6 pounds (3.9 kg)
Card Filler Panel	3.2 pounds (1.6 kg)
Cable Management Tray	0.6 pounds (0.27 kg)

Facility Requirements

To ensure correct operation of the ED-12000B, the facility where the switch is used must meet the following requirements:

- Power requirements for a physical inlet:
  - Power is provided by the power distribution system within the EC-1230B Connectrix equipment cabinet. See the power specifications for the EC-1230B in Appendix B.
- The power specifications listed in Table A-3 on page -5.
- An air flow of at least 350 cubic feet per minute, available in the immediate vicinity of the ED-12000B/EC-1230B.
- The environmental specifications listed in Table A-4 on page A-7.
- The electrical interference must be less than the levels stated in the standards listed under *Immunity* in Table A-5 on page A-8.

Power Specifications

WARNING

To remove power to the ED-12000B, disconnect both power cables.

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 following power specifications in Table A-3 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 A-3 Power Specifications

Specification	Value
Power cords	Two EMC power cords (038-002-736) are provided with each ED-12000B in the EC-1230B cabinet to connect to the PDUs within the EC-1230B cabinet to the power receptacles on the ED-12000B chassis.
Total power available from each power supply	1 KW
Input voltage	200 - 240 VAC Note: System can operate with three-phase or single-phase power utility installation.
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/hr 128 ports: 1960 Watts, 6700 BTU/hr

Table A-3 Power Specifications (*continued*)

Specification	Value
Maximum in-rush current per power cord	40 Amps Peak, 1/2 cycle
Input line protection	Thermal circuit breaker
Power supply dimensions	2.74 in. wide, 4.86 in. high, 13.50 in. long

Environmental Requirements

The following table lists the environmental operating ranges for the ED-12000B. The requirements for non-operating conditions are also provided for acceptable storage and transportation environments.

Table A-4 Environmental Requirements

Condition	Acceptable Range During Operation	Acceptable Range During Non-Operation
Temperature	0° to 40° Celsius[a] (32° to 104° Farenheit)	-25° to 70° Celsius (-13° to 158° Farenheit)
Humidity	5% to 85% RH noncondensing, at 40° Celsius	10% to 85% RH no-condensing, at 40° Celsius
Altitude	0 to 3 kilometers above sea level (0 to 10,000 feet altitude)	0 to 12 kilometers above sea level (0 to 39,370 feet)
Shock	4G, 11MS duration, half-sine wave	20G, 11MS duration, sq. wave
Vibration	5G, 0-3 kHz at 1.0 octave/minute	10G, 0-5 kHz at 1.0 octave/minute
Air flow	350 cu. ft/min. (0.00059 cu. meter/hr)	None required
Heat dissipation	64 ports: 3690 BTU/hr 128 ports: 6700 BTU/hr	Not applicable

a. The 0-40 degrees C temperature range is for the chassis. Individual components may have a higher range; for example, the 16-port cards and CP cards have a temperature range up to 75 degrees Celsius. Use the `tempShow` or `Fabric Watch` commands to show temperature status of all components.

General Specifications

The ED-12000B supports Distributed Name Server (DNS). The ED-12000B is compliant with United States and International safety and EMC Electromagnetic Compatibility standards. The following table lists the general specifications for the ED-12000B.

Table A-5 General Specifications

Specification	Description
Configurable port types	F_Port, FL_Port, and E_Port connections.
EMC (electromagnetic compatibility)	*Emissions:* An operating ED-12000B conforms to the EMC radiation levels specified by the following regulations: ◆ FCC Rules & Regulations, Part 15B, Class A level ◆ CISPR22 Class A ◆ EN55022 Class A ◆ VCCI Class A ITE ◆ AS/NZS 3548 Class A *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
System architecture	Non-blocking shared-memory
System processor	IBM Power PC 405GP, 200 MHz CPU
ANSI Fibre Channel protocol	FC-PH (Fibre Channel Physical and Signalling Interface standard)
Modes of operation	Fibre Channel Class 2, Class 3, and Class F
Fabric initialization	Complies with FC-SW 5.0
FC-IP (IP over Fibre Channel)	Complies with FC-IP 2.3 of the FCA profile

Table A-5 General Specifications (*continued*)

Aggregate I/O bandwidth	Per port: Up to 4 Gb/s, running at 2 Gb/s, full duplex Per 16-port card: Up to 32 Gb/s, all 16 ports at 2 Gb/s, full duplex
Port to port latency	Less than 2 microseconds with no contention (destination port is free)
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.

Data Transmission Ranges

Table A-6 provides the data transmission ranges for different cable types and port speeds.

Table A-6 Laser Data Transmission Ranges

Port Speed	Cable Size (microns)	Short Wavelength	Long Wavelength
1 Gb/s	50	1,640 feet (500 meters)	N/A
1 Gb/s	62.5	984 feet (300 meters)	N/A
1 Gb/s	9	N/A	6.2 miles (10 km)
2 Gb/s	50	984 feet (300 meters)	N/A
2 Gb/s	62.5	492 feet (150 meters)	N/A
2 Gb/s	9	N/A	10 km (6.2 miles) without an Extended Fabrics license. 50 to 100 km with an Extended Fabrics license.

16-Port Card Specifications

Port Specifications

The ports in the ED-12000B support full duplex link speeds at 2.125 Gb/s or 1.0625 Gb/s, inbound and outbound, automatically negotiating to the highest common speed of all devices connected to the port. Each port has a SerDes (serializer/de-serializer) 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 (short wave-length: 780-850 nm), and optical LWL (long wave-length: 1270-1350 nm), SFPs (small form factor pluggable media) and SFP-compatible cables. 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 (fabric ports), FL_Ports (fabric loop enabled), or E_Ports (expansion ports).

The ports meet all required safety standards. For more information about these standards, refer to *Regulatory Compliance* on page A-16.

CP Card Specifications

Memory Specifications

Each CP card has the following memory:

- Main memory: 128 MB SDRAM (32 Bits wide)
- Flash memory:
  - User flash: 16 MB of 16-bit wide memory, stored in two 8MB banks
  - Compact flash: 256 MB, partitioned in two 128 MB sections
- Boot flash: 512K bytes of 8-bit for system boot

The centralized memory maximizes the overall switch throughput by guaranteeing full transmit and receive bandwidth to all Fibre Channel ports at all times.

Battery Specifications

The CP card has a lithium carbon-monoflouride coin cell battery.

Table A-7 CP Card Battery Specification

Type	Specification
Rayovac BR1225	3.0 volt, 50 mAh

WARNING

Do not attempt to replace the real time clock (RTC) battery on the CP card. There is danger of explosion if the battery is incorrectly replaced. Contact EMC, since the battery must be replaced with the same type of battery as recommended by the manufacturer, and must be disposed of according to the manufacturer's instructions.

Terminal Serial Port Specifications

Each CP card provides a Terminal Serial Port with a DB-9 connector with an RS-232 signal subset (see Figure 2-5 on page 2-20).

For dust and ESD (electrostatic discharge) protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not in use.

The Terminal Serial Port can be used 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 pin outs listed in the following table.:

Table A-8 Terminal Serial Port Pin Outs

PIN	Signal	Description
1		
2	TxData	Transmit Data
3	RxData	Receive Data
4		
5	GND	Logic Ground

Table A-8 Terminal Serial Port Pin Outs *(continued)*

PIN	Signal	Description
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 (see Figure 2-5 on page 2-20).

For dust and ESD (electrostatic discharge) protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not in use.

The modem port can be used for attaching a modem to each CP card. The ED-12000B detects modems only during the power-on or reboot sequences, and automatically initializes them for operation. If modems are connected to an operating switch, a power on/off cycle, reboot, or fast reboot is required in order to detect the modem(s).

Customers should connect a *Y* cable on the telephone line to each modem. The active CP card answers on the first ring and the standby CP card answers on the 7th ring if the active CP card has failed to answer.

Table A-9 Modem Serial Port Pin Out

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

Table A-9 Modem Serial Port Pin Out (*continued*)

PIN	Signal	Description
7	RTS	Request to Send
8	CTS	Clear to Send
9	RI	Ring Indicator

POST and Boot Specifications

The ED-12000B performs POST by default each time the chassis is powered on (*cold boot*) or the ED-12000B is rebooted. The ED-12000B can be rebooted using the `switchreboot`, `reboot`, or `fastboot` commands. The `fastboot` command reboots the switches without running POST. A CP card failover event results in a reboot for the affected CP card.

POST

POST includes a number of diagnostic tests. Test results can be monitored through LED activity, the error log, or command-line interface. POST requires a minimum of three minutes to complete (time may vary depending on devices connected to ED-12000B).

POST includes the following steps:

1. Preliminary POST diagnostics are run.
2. Operating system is initialized.
3. Hardware is initialized.
4. Diagnostic tests are run on a number of functions, including internal connections and circuitry, port functionality, ability to send and receive frames, all aspects of memory, parity, statistics counters, and correct serialization.

Boot

Boot completes in a minimum of three minutes if POST is run:

1. Universal port configuration is performed.
2. Links are initialized.
3. Fabric is analyzed. If any ports are connected to other fabric elements (switches), the switch will participate in a fabric configuration.
4. The switch will obtain a domain ID and assign port addresses.
5. Unicast routing tables are constructed.
6. Normal port operation is enabled.

Regulatory Compliance

FCC Warning (USA only)

This equipment has been tested and complies with the limits for a Class A computing 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 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 the user's own expense.

VCCI Statement

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

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。

CE Statement

WARNING

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.

The standards compliance label on the ED-12000B contains the CE mark which indicates that this system conforms to the provisions of the following European Council directives, laws, and standards:

- 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.
- EN50082-2/EN55024:1998 (European Immunity Requirements)
  - EN61000-3-2
  - EN61000-3-3/JEIDA (European and Japanese Harmonics Spec)

Canadian Requirements

This class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations, ICFS-003.

Cet appareil numerique de la classe A respecte toutee les exigences du Regiements sur le material brouilleur du Canada, NMB-003.

Laser Compliance

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.

CAUTION

Use only optical transceivers that are qualified by EMC and comply with the FDA Class 1 radiation performance requirements defined in 21CFR Subchapter J, and with IEC 825-1. Optical products which do not comply with these standards may emit light that is hazardous to the eyes.

RTC Battery

WARNING

There is danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type of battery recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions. EMC will replace the CP card, if needed.

Electrical Safety

WARNING

To remove all electrical power from the ED-12000B, disconnect both power cables.

Connect the power cable only to a grounded outlet.

WARNING

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.

Regulatory Certifications

The ED-12000B is certified for the safety and EMC (electromagnetic compatibility) specifications listed in Table A-10.

Table A-10 ED-12000B Regulatory Certifications

Country	Safety Specification	EMC Specification
Canada	CSA 22.2 No. 60950 Third Ed.	CSA C108.8 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)	
Korea	사용자 안내문 : A 급기기 이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.	

Table A-10 ED-12000B Regulatory Certifications (*continued*)

Country	Safety Specification	EMC Specification
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.	
European Union (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom)	EN 60950:92 +A1:93+A2:93+A3:95+A4:96+A11:97 73/23/EEC TUV (Germany only)	89/336/EEC EN 55022:1998 Class A EN60825-1:1994/A11, -2 EN 61000-4-2 Severity Level 3 for Electrostatic 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
Australia and New Zealand		AS/NZS 3548:1995 Class A (radio interference)

B

Product Specifications for the EC-1230B

This appendix provides the following information:

EC-1230B Cabinet

Physical Characteristics

Dimensions		Height: 74 in (188 cm)
		Width: 24.25 in (61.6 cm)
		Depth: 37 in (94 cm)
Weight		EC-1230B with no switches: 400 lbs (183.04 kg)
		Packing container: approximately 100 lbs (45.35 kg)
Acoustical Noise		65 dB "A" scale
Inclination		10° maximum (packaged)
Fiber Cables Supported		384 maximum
ED-12000B installable		2 maximum per cabinet

Power Requirements

Input power	Two 30-Amp dedicated circuits, 208 to 264 VAC, 47 to 63 Hz. Each PDU within the EC-1230B should be connected to its own power circuit independent of the other PDU's power circuit.
User-supplied Power Outlets (2)	Domestic: Russellstoll 9C53U2 or 9C53U2T
	International: Russellstoll 9C53U2T
Input Power Cords (2) from EC-1230B	Russellstoll 9P53U2T

Operating Environment

Temperature	32° F to 104° F (0° C to 40° C)
Relative Humidity	5% to 85% (non-condensing)
Maximum Altitude	10,000 ft (3,047 m)
Service Clearance Front	**Front:** 36 in (91.5 cm) minimum
	Rear: 36 in (91.5 cm) minimum
	Sides: None necessary

CAUTION

Although the above service clearances are necessary only when the unit is being serviced, you should always provide at least 6 inches (15.25 cm) of clearance in the front and 6 inches in the rear for air flow.

Stabilizer/Outrigger Brackets

Connectrix stabilizer/outrigger brackets (P/N 100-605-014) mount to the bottom front and rear of the EC-1230B cabinet to prevent tipping.

When the EC-1230B cabinet is positioned such that it is not immediately adjacent (within 2 inches) to another equipment cabinet, the stabilizer/outrigger brackets must be positioned in their outermost position. (Refer to Figure B-1.) If the cabinet is positioned within 2 inches of another equipment cabinet, the outrigger brackets can be positioned in their innermost position.

Any side of the EC-1230B cabinet that is not within 2 inches of another equipment cabinet should have that side's outriggers positioned in the outermost position. These rules apply not only for initial installation, but also if the EC-1230B switch/director configuration is altered at a later date.

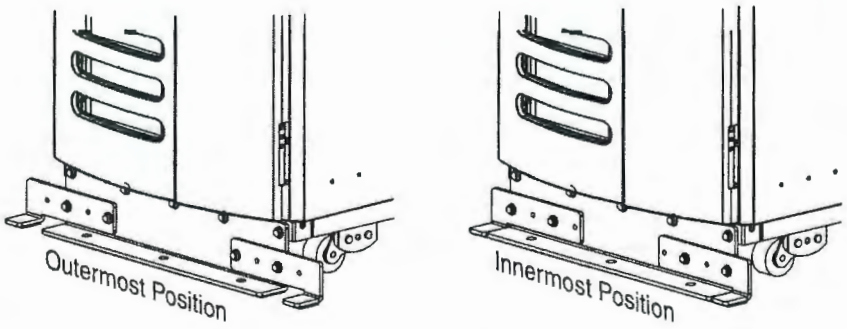


Figure B-1 Stabilizer/Outrigger Bracket Positions

Figure B-1 shows the front of the cabinet. Installation of the rear brackets is similar.

CAUTION

EMC recommends keeping the Connectrix Stabilizer / Outrigger brackets , P/N 100-605-014, on the EC-1230B cabinet at all times. When the cabinet is positioned such that it is not immediately adjacent (within 2 inches) to another equipment cabinet, the stabilizer bracket outriggers must be positioned in their outermost position. If the cabinet is positioned within 2 inches of another equipment cabinet, the outrigger brackets can be positioned in their innermost position. Any side of the EC-1230B cabinet that is not within 2 inches of another equipment cabinet should have that side's outriggers positioned in the outermost position. These rules apply not only for initial installation, but also if the EC-1230B switch and/or director configuration is altered at a later date.

Regulatory and Agency Certifications

- **Safety:** UL, CSA, IEC (CB), TUV
- **EMI:** FCC Class A, CE-Marking (IT Equipment Class A), VCCI, ICES-003, AS/NZS 3548 (Ctick), and BSMI Class A

C

Troublshooting and Diagnostics

This appendix contains the following sections:

Overview

The ED-12000B includes a number of diagnostic aids to assist with troubleshooting, including LED indicators on the hardware, commands that display current status, diagnostic tests for hardware and software, and error messages. In addition, a number of managing and monitoring features are available for purchase, including Fabric Manager, Web Tools, Fabric Watch, and Performance Monitoring.

If the ED-12000B does not behave as expected, the following steps can be taken to diagnose the problem:

- Check the LEDs and refer to the LED tables in Table 2-1 on page 2-18 for interpretation and recommended actions.
- Review the results of the last POST (power-on self-test) run by the ED-12000B (see *Interpreting POST Results* on page 2-27).
- Review the error logs (refer to the *Diagnostic and System Error Message Reference* and the *Fabric OS Procedures Guide* for more information).
- Enter the **sensorshow** command to determine the status of the hardware components.
- Run diagnostic tests (see *Diagnostic Tests* on page C-7).
- Reboot the relevant logical switch or power the entire chassis off and on.

If the problem is still unresolved after these steps, contact your support provider. The information required by your support provider in order to provide assistance is listed under *Reporting a New Problem* on page E-6.

Troubleshooting the ED-12000B

Table C-1 provides a list of issues, possible causes, and recommended actions.

Table C-1 Troubleshooting the ED-12000B

Issue	Possible Causes	Recommended Actions
Entire **chassis powers off** automatically.	Inadequate power supplies to support the installed components.	Add the required number of power supplies. A minimum of two are required to power a completely loaded chassis.
Several or all **components are not operating**.	◆ One or both power cables may not be connected to a live source. ◆ One or both AC power switches may be off.	◆ Ensure that both power cables are connected to live outlets. ◆ Ensure both AC power switches are on (AC switches light up green when on).
Serial connection is faulty or serial port logs have incorrect or missing information.	◆ Serial cable not connected correctly. ◆ Terminal emulator application parameters are not set correctly. ◆ Serial port may be incompatible (only RS-232 is supported) ◆ Pins on the serial cable or serial port may be damaged.	◆ Ensure cable is firmly connected to workstation computer and to switch. ◆ Ensure the terminal emulator application is configured as follows: 9600 bits per second, 8 databits, no parity, 1 stop bit, no flow control. ◆ Ensure switch is connected to an RS-232 port. RS-423 serial ports may experience difficulties due to corner-case incompatibilities of the standards. ◆ Remove the cable and inspect the pins on the cable and in the serial port. Do not reinstall if the pins on either component have any visible damage, as this could damage the pins on the other component. Replace components as required.

Table C-1 Troubleshooting the ED-12000B (continued)

Issue	Possible Causes	Recommended Actions
Modems are not detected by switch.	◆ Modems were connected after switch was powered on. ◆ Modems are connected to the wrong ports on the CP cards. ◆ Modems are not correctly configured. ◆ Pins on the modem cable or modem port may be damaged.	◆ Reboot the CP card(s) to which the modem(s) are connected. ◆ Ensure modem cables are connected to the ports labeled "RS232" (the serial ports intended for terminal use are labeled 10101). ◆ Verify modems are configured as described in Appendix D. ◆ Remove the cable and inspect the pins on the cable and in the port. Do not reinstall if the pins on either component have any visible damage, as this could damage the pins on the other component. Replace components as required.
Ethernet link speed is different than expected or a link cannot be established.	There may be a conflict with the ethernet link speed negotiation set up by the network.	Specify the ethernet link speed by entering the `ifmodeset` command. For more information about ethernet connectivity to the ED-12000B, refer to the *Fabric OS Reference Manual*.
Configuration data is inaccurate or cannot be accessed.	◆ Chassis was powered off then on while WWN card was uninstalled or failed. ◆ One or both logical switches were rebooted while WWN card was uninstalled or failed.	◆ Install an operational WWN card and power system off and on again. ◆ Same as above.
IP address or **domain ID** conflict during initial set up.	One or both logical switches were connected to the fabric before being configured.	Configure switches as described in this manual and the *Fabric OS Procedures Guide*.

Table C-1 Troubleshooting the ED-12000B (continued)

Issue	Possible Causes	Recommended Actions
LEDs on one or more components are changing rapidly or do not indicate a healthy state.	◆ Switch may be booting or running POST. ◆ Beaconing may be on for an entire logical switch or for individual components. ◆ Individual components may have failed. ◆ Pins on the components may be damaged.	◆ Verify that boot and POST are complete. The ED-12000B requires a minimum of three minutes after power-on to complete POST. ◆ Determine whether beaconing is on by entering the **switchshow** command and determine whether switch beaconing or blade beaconing are on. ◆ Refer to the LED tables in *LEDs on the 16-Port Card* on page 2-16 for interpretation and recommended actions. ◆ Remove component from chassis and inspect pins on component and inside chassis. Do not reinstall if pins on either component are visibly damaged, as this could damage pins on other component. Replace parts as required.
None of the **LEDs** on an individual component are lit.	◆ Component may not be seated correctly. ◆ Component may have failed.	◆ Ensure switch has power and component is firmly seated. If problem continues, run the **sensorshow** command to determine component status (see *Environmental Status and Maintenance Commands* on page 4-4). If component is a CP card or port card, enter the **slotshow** command to determine status. ◆ Replace component as necessary.
CP cards are failing over frequently.	◆ CP card is attached to an ethernet with high traffic loads ◆ Chassis is overheated.	◆ Remove switch from high traffic Ethernet segment (or upgrade to v4.0.2d or higher level of Fabric OS). ◆ Enter **sensorshow** command (see *Environmental Status and Maintenance Commands* on page 4-4) to check internal temperature. If components are overheating, shut down port cards as necessary to return the temperature to operating range

Table C-1 Troubleshooting the ED-12000B (continued)

Issue	Possible Causes	Recommended Actions
One or more **port cards** have either shut down or failed POST as indicated by the error log.	◆ Port cards may be overheated. ◆ Port card may be faulty. ◆ Pins on the card or on the backplane (inside the slot) may be damaged.	◆ Enter the **sensorshow** command (see *Environmental Status and Maintenance Commands* on page 4-4) to check the internal temperature readings. If components are overheating, shut down port cards as necessary to return the temperature readings to the operating ranges. ◆ Enter the **slotshow** command to determine status. For more information enter the **diagdisablepost** then the **slotpoweron [slot number]** command. Resolve the source of the problem or replace the card as required. ◆ Remove card from chassis and inspect pins on card and on backplane inside slot. Do not reinstall if pins on either component are visibly damaged, as this could damage pins on other component. Replace components as required.
An individual **component is not operating** as expected.	◆ Component may not have power or may not be firmly seated. ◆ Pins on the component or the backplane may be damaged. ◆ The component may have failed.	◆ Ensure component is receiving power (power LED should be lit) and component is firmly seated. ◆ Remove component from chassis and inspect pins on card and inside chassis. Do not reinstall if pins on either component are visibly damaged, as this could damage pins on other component. Replace parts as required. ◆ Enter the **sensorshow** command to determine component status (see *Environmental Status and Maintenance Commands* on page 4-4). If component is a CP card or port card, enter the **slotshow** command to determine status. Replace component as necessary

Diagnostic Tests

Diagnostic tests are automatically run during POST to check the status of the switch. Any error messages generated during POST are sent to the error logs and to the serial console, if connected.

Diagnostic tests can also be run manually to test and troubleshoot the hardware and the firmware, including internal connections and circuitry, transceivers, and port cables. However, diagnostic tests are generally intended for use by support personnel.

Diagnostic error messages do not necessarily indicate that the switch requires maintenance.

Each diagnostic test can be implemented by entering the related command through a telnet or serial session. For a list of diagnostic tests and commands, refer to the *Fabric OS Procedures Guide*.

All diagnostic tests are run at link speeds of both 1 and 2 Gbit/sec, and may temporarily lock the transmit and receive speeds to a specific speed. Some diagnostic tests require interconnecting the ports to each other or using loopback plugs. If ports are interconnected, the media (cables and transceivers) at each end of the connection must be of the same type. For example, short wavelength media must be connected to short wavelength media, and likewise with long wavelength media and copper media.

For more information about diagnostic tests and how to run them, refer to the *Fabric OS Procedures Guide* and the *Fabric OS Reference*. For information about diagnostic error messages, refer to the *Diagnostic and System Error Message Reference*.

D

Setting Up and Installing Modems

This appendix contains the following sections:

Overview

Each CP card in the ED-12000B contains a modem serial port for connection to a Hayes-compatible modem. The modem serial ports are wired as standard DTE ports and have the same command, log in capabilities, and operational behavior as the terminal serial ports. However, asynchronous informational messages and other unsolicited text are not sent to the modem ports. No additional software is required to use modems with the ED-12000B.

The ED-12000B detects modems only during power-on, reboot, or a CP card failover sequence. Setting up the modems before powering on the ED-12000B is recommended.

For increased security, any active modem sessions are automatically disconnected if the modem cable is disconnected.

For optimal security, disconnect the modem cable when it is not in use.

High Availability

High availability of the modem connection can be ensured by connecting a separate modem to each CP card, and then connecting both modems to a shared telephone line, as shown in Figure D-1. This ensures an available telephone connection to the active CP card even if a failover occurs; however, it is necessary to log back in after a failover. When both CP cards are connected to a shared telephone line, callers are automatically dialed into the active CP card, which 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 login to proceed.

If a modem connection is set up, connecting a modem to each CP card is recommended.

Location of Components

Figure D-1 illustrates the location of the modem serial ports and the supported set up.

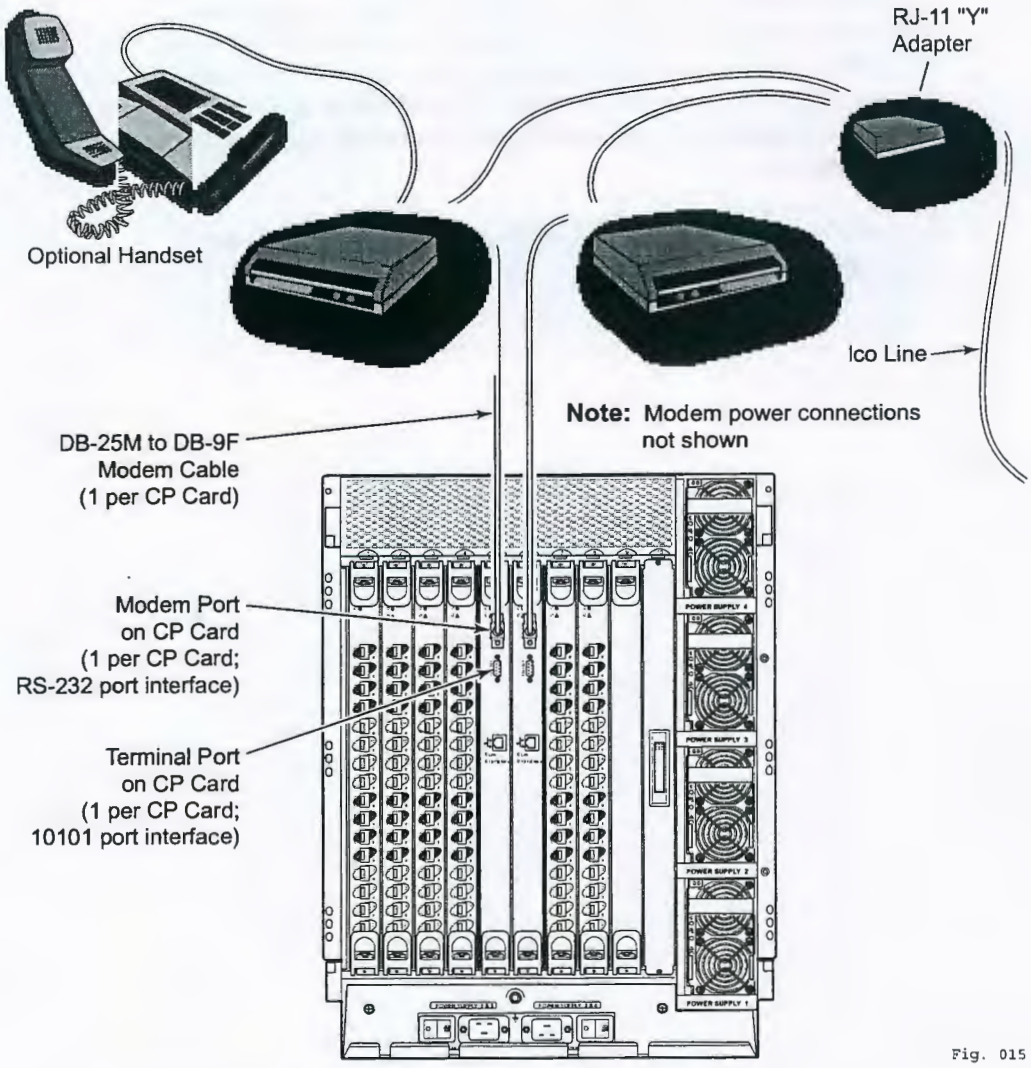


Figure D-1 ED-12000B With Two Modems Connected

Connecting Modems to the ED-12000B

Setting up the modems before powering on the ED-12000B and connecting it to the fabric is recommended.

The following items are required to set up two modems to work with the ED-12000B:

- 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 (3 total connections)
- One analog telephone line

CAUTION

Powering off the ED-12000B before connecting cables to the modem ports is recommended.

To connect modems to the ED-12000B:

1. Optional: Power off the ED-12000B.
2. Set up the two modem units and corresponding power connections.

   Do not power on the modems until all cables are attached.

3. Connect the modem cables to the modems and to the ED-12000B RS-232 modem ports, as shown in Figure D-1.
4. Connect the telephone "line" inputs on the modems to the RJ-11 "Y" connector.
   This effectively places both modems on a single telephone line.
5. Optional: Connect a telephone handset to one of the "phone" connections on the modems, as shown in Figure D-1.
6. Connect the "Y" adapter to an appropriate analog telephone line, and document the dial-in number for later use.
7. Power on the modems and verify that the Modem Ready indicator illuminates on both units.

8. Power on the ED-12000B, or reboot if it was not powered off during the previous steps.
   This allows the ED-12000B to recognize the modems.

Setting Up a Remote Modem System

After the modems are connected, 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.

This procedure is only required if a dial-out modem facility is not already available for testing the ED-12000B modem connections.

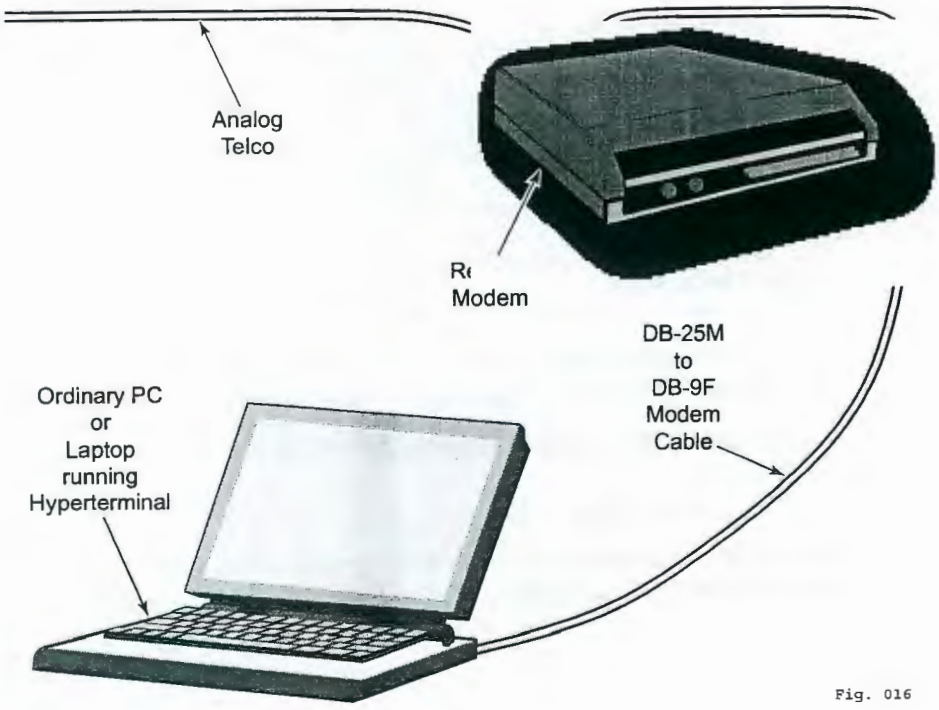


Figure D-2 Remote Modem Setup

To set up the optional remote modem:

1. Connect the remote modem to the workstation, as shown in Figure D-2.
2. Disable any serial communication programs running on the workstation (such as a synchronization program for a PDA).

3. Launch the terminal emulator application and configure as described below.

   - For Windows 95, 98, 2000, ME or NT, or TERM in a Unix environment, enter the following parameters:

Parameter	Value
Port Speed (bits per second)	115200*
Data Protocol	Standard EC
Compression	Enabled
Flow control	Hardware
Databits	8
Parity	None
Stop bits	1
Modulation	Standard

   * Port usually defaults to highest speed supported by modem, then may negotiate for slower speed.

   - For most UNIX systems, enter the following string at the prompt:

```
tip /dev/ttyb -9600
```

4. Follow the modem manufacturer's instructions for setting up and verifying modem operation.

Verifying the Modem Connection

This section provides information about how to verify that the modems are correctly connected.

This procedure requires either a telco system to dial-in to the modems or a terminal emulation program on a laptop or workstation that has an attached modem. The instructions for setting up a remote modem with a terminal emulation program is provided under *Setting-Up a Remote Modem*.

To verify the modem connection:

1. Verify that both modem cables are firmly connected.
2. Power-on the modems, if not already on.

   The modems must be powered on and operational before the ED-12000B is powered on, to allow the ED-12000B to detect the modems during boot.

3. Power-on the ED-12000B, if not already on.
4. Verify that both modems indicate they are ready by illuminating their "Clear to Send" (CS), "Terminal Ready" (TR), and "Modem Ready" (MR) indicators. If this does not occur ensure that the modems are connected to a power source and are powered on, and check all modem cable connections.
5. Verify that POST is complete on the ED-12000B (a minimum of 3 minutes).
6. Dial-in to the telephone number assigned to the ED-12000B, using a telco system to dial-in to the modems or the setup described in *Setting-Up a Remote Modem*.
7. Observe the modem lamps: the Ring Indicator should flash briefly as the telephone rings. If the Ring Indicator does not flash on both units, recheck the incoming telephone lines to the modems.
8. Verify that after one ring, the modem associated with the active CP card (usually in slot 5), illuminates the "Off Hook" (OH) indicator on the modem, and a login prompt is presented to the remote client.
9. Log into the switch from the remote client as Admin.

If the Off Hook lamp illuminates on the standby CP card modem, recheck the modem cable connection to the active CP card.

10. Log out of the modem session.
11. Remove the telco connector from the active CP card modem, leaving the standby CP card's telco line connected to the "Y" connector (see Figure D-1).

    The modem session is automatically disconnected if the modem cable is detached while a session is active.

12. Dial-in to the telephone number assigned to the ED-12000B, as described in Step 6.
13. Observe the modem lamps: the Ring Indicator should flash only on the modem connected to the standby CP card.
14. Verify that after seven rings, the Off Hook indicator on the standby CP card modem is illuminated. A login prompt is presented to the remote client, and a message confirms that the standby CP card is being logged into. You can now log in or disconnect the session as desired.
15. Reconnect the telco connector to the active CP card modem.

    The ED-12000B modems are now ready for use.

Advanced users can use the `hafailover` command to further evaluate the attached modems.
The ED-12000B requires approximately 5 minutes after a failover or reboot to set up the modems.

E

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure E-1).

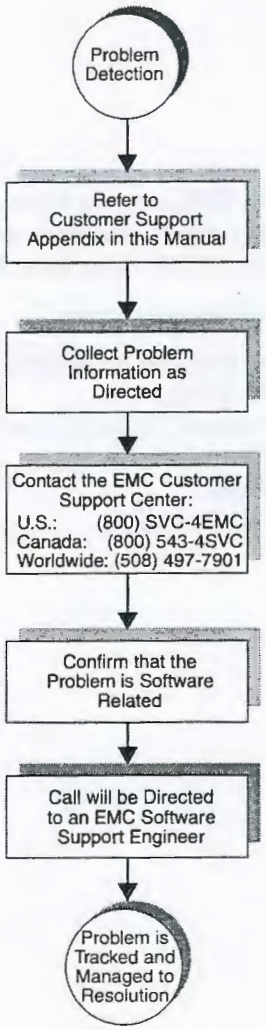


Figure E-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink Web site at:

`http://powerlink.emc.com`

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 Fibre Channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology*.

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch*.

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput*.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 tTlnet 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 Bit error rate. Tthe 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 See *Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*

CP Card Control processor card. The central processing unit of the ED-12000B, which contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*.

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data

communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and

application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

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.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.

FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and

Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.

I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode .

See also *Nonparticipating Mode* and *Participating Mode.*

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit.*

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL.*

M

Media See *Transceiver.*

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port.*

Multicast The transmission of data from a single source to multiple specified 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 meters between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port.*

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of Electrical Industries Association (EIA) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for

transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector, DCE 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. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.

- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

Index

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ECT
CPL - AC

ANEXO SWITCH TIPO 03
PARTE 2

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

EMC²
RELEASE NOTES

Connectrix B Fabric Manager
Version 4.0.1

Release Notes
P/N 085090697
Rev A01

6/23/03

These release notes contain supplemental information about EMC Connectrix B Fabric Manager, version 4.0.1. Topics include:

For more information on Connectrix B Fabric Manager, refer to the *Connectrix B Fabric Manager User Guide*.

General Information

Connectrix B Fabric Manager Manager (hereafter called Fabric Manager) is a powerful application that manages multiple EMC Connectrix B-Series and Brocade SilkWorm® switches and fabrics in real time. In particular, Fabric Manager provides the essential functions for efficiently configuring, monitoring, dynamically provisioning, and managing SAN fabrics comprised of EMC Connectrix B-Series switches as well as switches from the Brocade Silkworm family.

Through its single-point SAN management platform, Fabric Manager facilitates the global integration and execution of management tasks across multiple fabrics-thereby lowering the overall cost of SAN ownership. As a result, it provides a flexible and powerful tool optimized to provide organizations with rapid access to critical SAN information.

In addition, Fabric Manager is tightly integrated with other EMC Connectrix B-Series and Brocade SAN management products, such as Web Tools and Fabric Watch. Organizations can also use Fabric Manager in conjunction with SAN and storage resource management applications as the drill-down element manager for a single or multiple fabrics.

Highlights

- Provision, monitor, and administer large numbers of switches and multiple SAN fabrics with greater efficiency
- Perform management tasks across multiple devices and fabrics as a single management operation
- Intelligently group multiple switches or ports to facilitate aggregated management
- Visualize and track changes to SAN configuration and state information through multiple views at multiple levels of detail
- Launch Fabric Manager from other enterprise management applications as the "element manager" for the fabric or multiple fabrics
- Track SAN assets by using detailed table views that can be exported to a spreadsheet
- Discover details about devices logged into the fabric, including HBA asset information

- View the SAN layout through a topology map that specifies ISL, switch, and device details
- Identify, isolate, and manage SAN events across large numbers of switches and fabrics

New Features

The following information highlights the differences between Brocade Fabric Manager 3.x and Connectrix B Fabric Manager 4.0.1 and is being provided for users familiar with the functionality found in Brocade Fabric Manager 3.x.

- Discovery
  - Discover all switches
  - Discovery of switches and fabrics through subnet scanning
  - Device information including FDMI data if available
  - Allows user to select if SAN elements will be displayed by WWN, domain/port ID, IP address or element name
  - Tree view of elements organized by fabrics, switch/port groups
  - Users can easily choose from 1 of 8 different predefined views
  - Drill down ability allows detailed element information to be displayed
  - Actions on elements can be launched directly by the right mouse button
  - Intelligent handling of fabric segmentation and merging
- Fabric/Switch/Port administration
  - Web Tools can be invoked for a specific switch to do element management (such as switch administration, Fabric Watch, performance monitoring)
  - Fabrics, switches and ports can be named
  - Switches and ports can be enabled/disabled
  - Switch login credentials are saved for a specific session so that the user must authenticate themselves only once for a switch. The same credentials can be used across multiple switches
  - Maintain sessions once authentication with a switch has succeeded, including managing session expiration

- Time synchronization across fabrics

- SAN Element grouping
  - SAN elements such as switches and ports can be aggregated into groups. Administration of these groups (such as enable/disable) can be done en-masse. Elements can be in multiple groups
  - Groups can be nested to arbitrary depths
  - Groups can be exported and imported thus allowing them to be shared across multiple Fabric Manager client instances
- Firmware/Configuration Download

Does not apply to EMC Connectrix B Series switches. Please contact yuor EMC Service Representative for firmware updates.

  - Allows firmware download across fabrics to all switch types/firmware versions
  - In-band firmware download to HBAs (Emulex)
  - Allows configuration upload/download across fabrics to all switch types/firmware versions
- Sequenced Reboot
  - This feature enables creating and saving of a sequence of rebooting groups of switches in a fabric in a pre-determined order
  - These sequences can be executed with different inter-sequence delays and with checks for fabric stability after a reboot
- Fabric Checking
  - Ability to retrieve and save the current state of a fabric with respect to switch membership (as a baseline for example)
  - Ability to retrieve and save complete ISL information on the fabric (including trunking information)
  - Detect and display differences between the current and the saved states according to status levels set by the user
  - Fabric merge checking looks for merge (in)compatibility across zoning, security and similar potentially conflicting areas
- Topology

- Use ISL and Fabric information (as populated in the object model) to graphically render various SAN elements and their relationships/links

- Events and Status
  - Display a list of events for each switch
  - Propagate the events of an element (such as switch) up to the fabric or user-defined switch group to allow aggregation of event data
  - Using sources such as ISL checking, fabric checking, switch status and connectivity, provide reasons for various statuses
  - The reason field in conjunction with the event information is displayed together to make it easier to troubleshoot problems in the fabric
  - Monitor and display related events
  - Propagate status upwards within groups (such as fabrics or user defined element groups). The status of a fabric can be seen even when the FM application is iconified
- At-A-Glance and tabular views
  - There are 13 levels of At-A-Glance hierarchical views from a device level up to a SAN level displaying aggregated data in user selectable/re-orderable/expandable items
  - These are dynamic, easily extendable views that can be configured to display different data from the fabric data model
  - They allow filtering based on element type and can cascade starting from any point in the fabric element tree
  - Portgrid is a specific table-view that enables a user to quickly see all the F-ports in the fabric and the devices that are attached to them
- Data polling
  - FM is a multi-threaded application that polls for information about various elements in the SAN at pre-determined intervals
- License management
  - Automate distribution of license keys to multiple switches in a SAN
- Persistence

- Fabric Manager will persist some application specific data (such as fabric/switch/port/group names, fabric/group memberships, reboot sequences, existing license keys) across sessions

- Call-home support
  - Client side GUI that allows a user to configure the conditions that will trigger a call-home action
  - Server monitors a user-configurable set of switches for changes/events in order to send a request for action based on configured parameters
- Context sensitive help pages

Requirements and Compatibility

This section includes requirements and compatibility for the Fabric Manager.

Host Support

- Windows 2000 Client and Server
- Solaris 2.7 Client with Windows 2000 Server
- Solaris 2.8 Client with Windows 2000 Server

Installation

Windows 2000 (FM Client and/or FM Server)

- Insert Fabric Manager CD into the CD Rom Drive
- The CD will auto-launch the Fabric Manager Installation Wizard
- Follow the installation instructions to complete the installation

Solaris (FM Solaris Client only)

Requires a Windows 2000 Server.

- Insert CD
- Navigate to Solaris folder
- Execute Install.bin

To Run

- FM server runs as a service on windows and is started automatically after installation.

- (Windows FM Client) Select Start > Fabric Manager > Fabric Manager.
- (Solaris FM Client) Navigate to FM install folder and execute "./startFabricManager".
- Enter the IP address of the FM server that is running on windows, providing login authentication (even if client is running on Solaris).
- Enter the IP address or name of a switch in the Address Field to start managing your Fabric.

Installation Notes

- Supported Operating Systems: Server: Windows 2000 Server or Professional only; Client: Windows NT Pro or Server, Windows 2000 Pro or Server, Solaris 7 or 8.
- If the Setup/Install GUI never comes up during install, run the DOS command "dxdiag" and make sure that the graphics tests run without error. If any DirectX files are missing or any diags fail, go to Microsoft's web site and upgrade to the latest version of DirectX.
- To find the domain name to use as the windows authentication domain that must be specified during installation, open a dos windows and type "set". The alias "USERDOMAIN" will indicate the active domain. If the client and server will reside on different Microsoft domains, both domains MUST have trusts established between each other, or FM will not be able to authenticate the client. The user should know which domain their systems are in, or check with their IT department. Also note that this domain is NOT the "internet" domain (as in corp.mycompany.com), it is the domain name Microsoft uses for authentication.
- The client software will poll the fabric information directly, so the client must be able to access each switch via an IP connection. Make sure the network environment does not have any proxy server or firewall between the client and the server and the switches. If one exists, ensure that proper rules are set up to allow access. In order to monitor switches for 'Call Home' events, only the server needs IP connectivity to the switches.
- If you have problems installing on a Solaris system you may be able to resolve it by making sure the recommended J2SE patches for Solaris java applications is installed. These patches can be found at:
  `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`

Use the appropriate one for your version of Solaris. Issues may also be encountered when using xwindows emulators from Windows to access the sun host.

- Java is keyed to whatever version your browser and/or switch needs for WebTools. Java JRE, however, is now embedded into FM install and may be a different version of java than what is already installed on the system. Use the following procedure to determine the java version in use for Fabric Manager:

  1. cd to C:\Program Files\Fabric Manager\jre\bin
  2. Run the DOS command "java -version" to determine the version of java in use.

- Before installing, check to make sure the system has the latest video drivers installed (to be safe, the user may also wish to upgrade to the latest DirectX drivers as well). Certain systems may crash with a "Blue-Screen" or the setup GUI may not startup-caused by an interaction between Java, Microsoft DirectX drivers, and the Video driver. The above crash/GUI issues have been resolved by upgrading the mentioned drivers and DirectX to the latest versions. The following link takes you to the page from SUN that mentions the issue (search on "blue screen"):

  `http://java.sun.com/j2se/1.4.1/relnotes.html`

- If Fabric Manager is installed on the same platform as an existing EMC Control Center Console installation, an attempt to uninstall the ControlCenter Console and subsequent reinstallation could fail. This is due to Java installation incompatibilities between the two products. The resolution to this situation may require multiple steps, as follows:

  1. Launch Internet Explorer. From the menu, select **Tools-Internet Options** and select the **Advanced** tab. Scroll down to the Microsoft VM section and verify that **Microsoft VM JIT compiler for virtual machine enabled** is the only virtual machine setting selected. If you have another installation of Java, you may have to deselect the JAVA (SUN) option.
  2. Attempt the reinstallation of the ControlCenter Console. If the download from the ECC Server host fails with a Java Exception in the browser window, proceed to Step 3.
  3. Verify that there are no pre-existing JRE or JDK installations on the host by going to **Start-Settings-Control Panel-Add/Remove Programs**. If one is found, close the

browser, remove the existing JRE/JDK, launch the browser, and then attempt the installation again. If no other separate JRE/JDK installations are found, you may have to uninstall Fabric Manager, reinstall the ControlCenter Console, then reinstall Fabric Manager.

Uninstall/Reinstall Issues

- To go from Brocade Fabric Manager v3.x to Connectrix B Fabric manager v4.x you can just run install and over-write the older version
- From v4.x to v4.x (same or newer version and Client/Server on same system) you can just run install and over-write the older version.
- After the Evaluation version is installed, users must upgrade to a licensed version within 60 days. The fully-licensed version requires an enabling key. If you do not have an enabling key, please contact your EMC Account Representative.

Changing User Settings After Installation

- For Domain: Edit

  `C:\FMServer\server\FabricManagerServer\conf\login-config.xml`

  and change the following to match the new domain name:

```
<application-policy name="Win32Procurator">
    <authentication>
        <login-module
   code="com.emc.procurator.mbeans.clientmanagement.WinNTLoginModule"
      flag="required">
      <module-option name = domain">emc</module-option>
```

- For Mail Server settings: Edit

  `C:\FMServer\server\FabricManagerServer\deploy\mail-service.xml`

  and change the following (3) lines:

```
<!-- Change to the mail server  -->
          <property name="mail.pop3.host" value="mail.emc.com" >

          <!-- Change to the SMTP gateway server -->
          <property name="mail.smtp.host" value="mail.emc.com" >

          <!-- Change to the address mail will be from  -->
          <property name="mail.from" value="markpcl@emc.com" >
```

The Fabric Manager Service must be restarted for the changes to take effect.

OS Requirements

The following table summarizes the versions of firmware and software that are supported in conjunction with this release:

	DS-8B and DS-16B SW2xxx	DS-16B2 SW3200 and SW3800	DS-32B2 SW3900	ED-12000B SW12000
General Compatibility	2.6.0c or later	3.0.2c or later	4.0.2 or later	4.0.0c or later
With Secure Fabric OS enabled Does not apply to EMC Connectrix B Series Switches.	2.6.1 or later	3.1.0 or later	4.1.0 or later	4.1.0 or later
Recommended adjacent to DS-32B2s or Silkworm 3900s running 4.1.0 or later	2.6.1 or later	3.1.0 or later	4.1.0 or later	4.1.0 or later

Obtaining Software Updates

Contact EMC Global Services for software updates and maintenance releases.

Documentation Addendums

The following note should be added to the *Connectrix B Fabric Manager User Guide,* v4.0. It should be added in the Introduction of Chapter 19, *Emulex HBA Firmware Download.*

Simultaneous firmware downloads to one or more HBAs on the same host, from multiple Fabric Manager Clients is not supported. Doing so will most likely corrupt the firmware on the HBAs, leaving the HBAs unusable.

Chapter 2, *Installing Fabric Manager,* on page 2-11, *Installing Fabric Manager Client,* should read as follows:

To install the Fabric Manager client, perform the following steps:

1. **Windows Environment:** Double-click the Windows folder from the Fabric Manager Installation CD-ROM.

   Solaris Environment: Click install.bin from the File Manager window that displays when you insert the Fabric Manager Installation CD-ROM.

2. Double-click the Install icon. The InstallAnywhere dialog runs, then the Fabric Manager installation wizard displays (see Figure 2-3 on page 2-3).

Support Limitations

Connectrix B Fabric Manager can be used to manage switch objects from the EMC Connectrix B-Series as well as those from the Brocade Silkworm family. The EMC Connectrix B-Series switches which can be managed from Fabric Manager are the: DS-8B, DS-16B, DS-16B2, DS-32B2, and the ED-12000B.

The switches from the Brocade Silkworm family which can be managed from Fabric Manager are the Silkworm: 2400, 2800, 3200, 3800, 3900, and 12000.

EMC does not restrict the use of Fabric Manager to fabrics comprised exclusively of EMC Connectrix switches. EMC will provide support for all of the functionality of Fabric Manager as documented in these *Release Notes* and in the *Connectrix B Fabric Manager User Guide*. This should not be construed to imply that EMC endorses the use of products not offered by EMC or that configurations not documented by EMC in the EMC Support Matrix (ESM) will operate properly.

EMC cannot respond to questions or provide support for products not offered by EMC or configurations that do not conform to the tested configurations found in the EMC Support Matrix.

EMC DS-8B and DS-16B and SilkWorm 2xxx Scalability Limits

Testing has demonstrated that SilkWorm 2000, DS-8B, and DS-16B switches should not be deployed in fabrics whose size exceeds 500 user ports (device ports). Such switches will not be supported in fabrics that exceed this size, regardless of Fabric OS version. For scalability and configuration rules regarding EMC Connectrix B-Series switches, consult the EMC Support Matrix.

Important Notes

Please see the Connectrix B Fabric Manager Users documentation Guide for full details on these features.

Area	Description
FDMI	FDMI issues: ◆ FDMI-capable HBAs must be connected to an FDMI-capable switch in order to get the FDMI functionality. ◆ FM-launch switch must be FDMI-capable in order to be able to "Refresh FDMI Info" by right clicking on the fabric in the tree. ◆ Currently, Emulex is the only vendor supporting FDMI for their HBA. The only platform they support is Windows 2000. Other platform support will be phased in over time. ◆ Emulex currently does not have a Solaris driver that supports the FDMI protocol. Only Windows 2000 drivers support FDMI at this time. ◆ FDMI is disabled by default on the Emulex HBA. You must enable FDMI by using either the "elxcfg" or "lputil" tool.
FICON	FICON testing is not supported in this release.
HBAnyware	HBAnyware does not support more than 8 HBAs in the same host. More than 8 HBAs in the same host causes intermittent Firmware Download failures, and can also cause the host to crash.
IBA Firmware Download	Emulex HBAnyware code does not run in a multi-threaded environment and is non-reentrant; therefore, simultaneous Firmware Downloads to multiple HBAs will corrupt the firmware.
HBA Firmware Download	When using Brocade API inside Fabric Manager to download firmware to the HBA, in come cases invalid firmware files are downloaded to the HBA. This causes the operation to report that it has finished successfully; however, the firmware is corrupted when rebooted.This is not a Brocade issue. The HBA does not discriminate and will load any files even if they are not to be loaded.

Area	Description
HBA Firmware Download	Firmware Download does not work for certain earlier and unsupported versions of HBA firmware, driver, and HBAnyware versions.Workaround: Use the latest versions of each (together) to correct this issue. The current version of Driver tested is V5-5.00a10-1 for Windows 2000 with firmware version 3.90a7. The current version of HBAnyware is included with this driver package.
ISL Threshold Overflow	ISL Threshold Overflow set for entire FM application - cannot set for individual switch links.
Polling intervals	Polling intervals: ◆ Name Server info — 30 secs ◆ All other functions — 15 secs
Security policy	The maximum number of members that can be added at one time to a single DCC policy is 125.
Upgrading Fabric Manager	**Problem:** If you try to install the Fabric Manager server immediately after you close the Fabric Manager client, the installer indicates that the port is in use. This happens because when you close a Fabric Manager client program, the Fabric Manager server takes about 4 minutes to free the connection port. **Workaround:** Wait about 4-5 minutes after closing all clients before you install the Fabric Manager server.

Defect Lists

This section contains a list of defects:

- Acronyms Used in the Defects Lists
- Outstanding Software Defects
- Fixed Defects

Acronyms Used in the Defects Lists

Following is a list of acronyms used to classify the defects in the outstanding adh closed defects lists:

Acronym	Definition
PRNT	Printing
SUBSC	Subnet Scan
AAG	At-A-Glance
ELIC	E-Licensing
PORT	Port View
LIC	License Management
TOPO	Topology View
BKEND	Requires backend fix
SEC	Security
3600	3600
SCAL	Scalability
DSCV	Discovery
GRPS	Groups (not Switch Groups)
CFG	Configuration upload/download; baseline
FWDL	Firmwaredownload
RBT	Reboot
MKGCK	Merge Check/Zone Merge

Acronym	Definition
USE	Usability
INST	Install
FABCK	Fabric Checking
ISLCK	ISL Checking
GEN	General
FICON	FICON
STRESS	Stress tests
HELP	User Guide/Online Help
HBAFW	HBA Firmware Download
SERV	FM Server
CALL	Call Home Client/Server

Open Defects in Fabric Manager 4.0.1

Table 1 lists open defects which are still under active investigation to be fixed in Fabric Manager. EMC does not formally close a defect until verification of the fix has been completed. Hence, fixes awaiting verification, or in the middle of verification, are still nominally considered "open".

Defects may also appear in this list if they have been seen once, but have eluded re-creation during additional weeks of testing. Such defects will be flagged as "Tracking". If they cannot be reproduced, they will eventually be closed. Should a defect closed with Tracking status recur, it will be reopened. Finally, some defects in this list appear as a result of aggressive "Stress to Fail" testing, which creates scenarios unlikely to occur in customer deployment. The bottom line is that customers are unlikely to encounter defects in this list, even though they are still officially considered "open".

Table 1 Defects Open in Fabric Manager 4.0.1

Defect ID	Severity	Summary
000025050	Medium	**Summary:** 30% of the time, under Switches view, some fields in Fabric column are corrupted after doing sequence reboot on multiple groups. **Symptom:** 30% of the time, when doing the Reboot/Fastboot on core switches, "Fabric" column under "Switches" view will be corrupted after Reboot/Fastboot. Some incorrect IP addresses will be filled in Fabric column. **Workaround:** Go to "Actions" and select "Refresh"; this will bring all the data back. **Customer Impact:** This happens in large fabrics and can be worked around by refreshing the data. Probability is low and impact is low. **Probability**: Low This defect was recently written against a previous release of Fabric Manager and was determined to still exist in current code, so it has been transferred to the current code base.
000025260	High	**Summary:** FM Client runs out of memory after switchDisable/switchEnable on core switches. **Symptom:** Using CLI switchDisable/switchEnable run on two core switches for an equivalent of 8-9 times with a 10 minute interval between each disable/enable will produce an OutOfMemory Error for the FM Client. At this point, the UI stops responding and the application will hog 100% of the Client's CPU. If a user leaves FM open for this equivalent of time and generates the same amt. of switchDisable/Enable, it will occur consistently. **Workaround:** When performing switchDisable/Enable on core switches don't do this repetitively while leaving FM monitoring overnight. **Customer Impact:** This only happens in large fabrics while doing repetitive switch enable/disable on the core switches. It's a stress test that should not be seen in the field. **Probability**: Low

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000013334	Medium	**Summary:** Core-Edge layout when Expanding/Collapsing links percentage bar goes to 100% multiple times. **Symptom:** When expanding or collapsing all link bundles in Core-Edge layout Topology view, the status bar in the lower right-hand corner goes to and from 100% multiple times. On larger fabrics (20+ switches) when expanding or collapsing all link bundles since the status bar goes to 100% for every expansion/collapsing of link bundle this appears the application is hung or in a loop, which is not the case. Have to wait for all the link bundles to have been expanded or collapsed before the status bar is done going back and forth from 100%. **Workaround**: No workaround.
000013400	Medium	**Summary:** Nodes are repositioned after expanding/collapsing link bundles. **Symptom:** In any of the 3 Topology layouts, when expanding or collapsing link bundles sometimes switch nodes are re-positioned. Also a switch node will not only be re-positioned but will sometimes swap position with another switch node. **Workaround:** No workaround.
000015078	Medium	**Summary:** Moving nodes then re-laying out view in Tree layout sometimes causes nodes to overlap. **Symptom:** In Topology view Tree layout, sometimes after moving nodes then re-selecting Topology menu >> Layout >> Tree, the nodes will reposition themselves and sometimes will cause them to overlap each other. **Workaround**: Workaround is to move all the nodes so that they are all fixed. This bypasses the partial layout algorithm issues and still allows the user to determine where they want their nodes to be.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000020178	Medium	**Summary:** 'GEN: Devices' table showing entries after the switch, with devices connected, is disabled. **Symptom:** User will see this problem in FM when a switch that has devices is disabled. When this occurs, ports table in FM will show all ports to be 'U' ports, but 'Devices' table continues to show all devices. **Workaround:** No workaround exists.
000020299	Medium	**Summary:** Printing topology view from File >> Print in one page, does NOT include Legend in printout. **Symptom:** Printing a topology layout in One Page that originally does not fit the screen, causes the print out to make the lettering and graphics of the Legend to be very small and unreadable. **Workaround**: Zoom the Topology view so that it fits on the screen. Use the Snapshot feature to save the layout to a PNG graphics file. Then using a graphics program or web browser, print out topology from one of these applications.
000020529	Medium	**Summary:** Unable to test LDAP authentication scheme in the lab. **Symptom:** Ldap Authentication scheme is not supported for the Fabric Manager server. **Workaround:** Fabric Manager server provides no support for ldap authentication scheme.
000022515	Medium	**Summary:** Switch column in Event Log stuck at switchname no matter what user selects in ID field. **Symptom:** All the different views that are in the View Selection bar except for the Event view, support the ID Selector. When in Event view when changing the ID Selector from Name to IP/WWN/Domain ID nothing happens. **Workaround:** When gathering data from the Event view, correlate the Switch Name from the Event Table to IP/WWN/Domain ID. Remember the Switch Name, then change the view to Switches table, then match Switch Name to other switch properties.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000022698	Medium	**Summary:** Links did not reconfigure correctly in the core-edge topo mode. **Symptom:** Following a disruptive HA failover, ISL links connected to nodes may shoot out and become out of proportion in the topology view. **Workaround:** Whenever the ISL links that connect to the nodes become out of proportion, the user must select any of the ISL link styles and the topology layout issue will be corrected.
000022939	Medium	**Summary:** FM Server start script on Solaris should use init to start server process. **Symptom:** The Fabric Manager server product is not being supported for the Solaris platform. **Workaround:** Fabric Manager server feature is not being supported for the Solaris platform.
000023166	Medium	**Summary:** Unable to view merged db after removing conflicts. **Symptom:** Running Fabric Merge Check against 2 fabrics that have different Zoning databases and have Type mismatch conflicts. The Zone Merge Manager that appears when running Fabric Merge Check, the conflicts will be able to be resolved within the GUI but the Zone Merge Manager will not display a merged zoning database. Since the Zone Merge Manager cannot display the merged zoning database from the 2 fabrics, you have to cancel the operation and fix the conflicts outside of FM, for example in WebTools Zone Admin or CLI. **Workaround:** If this problem occurs, a user can go into the CLI or WebTools Zone Admin feature to resolve the conflicts.
000023934	Medium	

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000023938	Medium	**Summary:** Link shootout seen in topology, tree layout. **Symptom:** User will encounter this problem if a fabric is displayed in Topology Tree layout for extended periods of time, when the fabric is reconfiguring. **Workaround:** User can avoid the problem by avoiding displaying a large fabric in topology - tree layout for extended periods of time when the fabric is reconfiguring. User can recover from this problem by toggling between the two link styles (click on 'straight' linkstyle and toggle back to 'orthogonal' and the links layout correctly) or by collapsing and expanding the graph node.
000024167	Medium	**Summary:** Different Backup options in Win 2K & Solaris 8. **Solution:** Added the following note in the Configurations page, backup configs procedures: Backing up a Fabric or Zoning Configuration: • Select a switch or fabric to backup from the SAN Elements tab. • Log in to the switch or fabric. • Select Backup from the Actions menu. The "Backup Configuration" dialog displays. In a Solaris environment, you will see two extra buttons: Help and Update.These buttons are not related to Fabric Manager and should be ignored.
000024465	Medium	**Summary:** Unable to open multiple TXN key files simultaneously on Solaris. **Symptom:** Customer will encounter this problem in FM (only on Solaris), when trying to open multiple TXN key files simultaneously by selecting the files and clicking on 'Ok' button in the file chooser dialog. **Workaround:** In the file chooser dialog, select multiple TXN key files and double click on the selection.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000024701	Medium	**Summary:** Ports Switches and Devices Tables are blank. **Symptom:** A customer could encounter this issue if they are viewing the switches table while a large fabric is going through constant reconfigurations for a prolonged period of time. **Workaround**: If a customer encounters this problem, close and restart the application.Customer Impact: This is a stress test and should not occur in a customer SAN. **Probability:** Low
000024961	Medium	**Summary:** Misleading status posted when FWDL from multi-clients to same devices. **Symptom:** Simultaneous FWDL to HBAs from multiple FM clients to the same HBA would correctly posted "failed" on one client and "success" on the other. However, from HBAnyware, the firmware code of the device may still have the old version and never really upgraded. Also, it might permanently corrupt the firmware on the HBA, resulting in unusable HBA. **Workaround:** Initiate FWDL to HBAs from a single FM client only to one or more HBAs on the same host.
000025050	Medium	**Summary:** FIELD_CORRUPTED: 30% of the time, under Switches view, some fields in Fabric column are corrupted after doing sequence reboot on multiple groups. **Symptom:** 30% of the time, when doing the Reboot/Fastboot on core switches, "Fabric" column under "Switches" view will be corrupted after Reboot/Fastboot. Some incorrect IP addresses will be filled in Fabric column. **Workaround:** Go to "Actions" and select "Refresh"; this will bring all the data back.Customer Impact: This happens in large fabrics and can be worked around by refreshing the data. Probability is low and impact is low. **Probability:** Low

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025114	Medium	**Summary:** 2+2+24 & 2+10 SEC: Cannot bring up Security Admin in a 2+10 Security Enabled Fabric. **Symptom:** Error code -221 is returned if fabric has recovered from an unstable(reconfiguring) state upon bringing up Security Admin. If however, the fabric is in a usable non-reconfiguring state, the SecAdmin should be able to come up without any errors. Would recommend changing the Security Admin UI response on this from printing out -221 to the user- rather fabric is busy or fabric is unstable when it encounters the Unknown error. **Workaround:** Run Security Admin after fabric is in completely stable state and has not reconfigured for over 10 mins. due to a CP Failover or switchDisable/switchEnable event. **Customer Impact**: This occurs mainly in large, unstable fabrics using security and should not be seen in most customer configurations. **Probability:** Low
000025152	Medium	**Summary:** Switches not ghosted in tree when switch is powered down with Fabric Checking ON. **Symptom:** If a user powers down a switch that is part of a checked fabric, then they will encounter this issue. The switch will not be "ghosted" in the fabric tree or in any of the Fabric Manager views. Also no event will appear in the Fabric Manager events table indicating that the switch was removed from a checked fabric, although the switch will appear as unreachable, it will have a red status color and an event indicating that the switch is unreachable will be displayed in the events view. **Workaround:** If a user powers down a switch that is part of a checked fabric, then they will encounter this issue.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025217	Medium	**Summary:** Device view shows single entry if multiple duplicate Node WWNs appear in fabric. **Symptom:** In the Device table view, when a fabric has multiple devices that share the same Node WWN. Only one entry will be displayed for each unique Node WWN. This is also true for the Device At-A-Glance view. This causes a mismatch between the number of Device displayed between Device table view in FM and the Name Server table in Webtools/CLI. **Workaround:** Use Webtools Name Server or CLI command 'nsShow' to view a complete listing of Node WWNsCustomer Impact: We are working on redesigning these screens for the next release. It will be more apparent in FICON implementations. **Probability:** Low
000025472	Medium	
000025477	Medium	**Summary:** CALL: Reset says successful when FM Server has been stopped. **Symptom:** In the Call Home window, when clicking on the Reset button a successful message appears, if the client has a connection to the FM server or not. **Workaround:** If you want to refresh the Call Home window with the most current data from the FM Server rather than resetting back to what was originally retrieved from the server, close the Call Home window and re-open by clicking on Tools menu >> Call Home.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025512	Medium	**Summary:** AAG active zoning does not expand to show zones in cfg of 124 MB. **Symptom:** A user could encounter this issue when viewing fabrics with large zoning databases (more than 512 active zones in the configuration) in Fabrics-At-A-Glance. The active zoning configuration cannot be expanded to show its component zones with configurations of this size. Similarly, a user can also encounter this scalability issue if the number of attached fabric devices equals or exceeds 512 entries in the Fabrics-At-A-Glance for Devices. The Node WWNs for this large count of devices cannot be expanded and viewed in Fabrics-At-A-Glance. **Workaround:** Two workarounds available for the Zoning AAG and for the Device AAG views: ◆ Fabrics-At-A-Glance ZoningT • The active zoning link in Fabrics-At-A-Glance cannot be expanded if a user is viewing a fabric with an active zoning database of more than 512 active zones. Hence, there is no workaround when viewing zoning configurations of this size in Fabrics-At-A-Glance. • There is a workaround with the Zone Admin tool if a user spawns from the fabric Zone Admin-> Mixed Zoning -> Config tab where the Zoning information on a drill-down basis is available. Although this is more tedious, if a user drills down on individual zones and sums up the Switch Ports and Zone WWNs, it will equal the same number of Zones as that reported by AAG. ◆ Fabrics-At-A-Glance • Device ViewThe Devices link information in Fabrics-At-A-Glance view cannot be expanded in this view if the Fabric contains more than 512 device WWN entries. Only resolution is to switch to Devices View of the given Fabric(s) to discover the present device WWNs. **Customer Impact:** This is a large fabric issue with a workaround, not likely to occur in a customer SAN. **Probability**: Low

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025655	Medium	**Summary**: 142986 Switch Unreachable Status During Firmware Download Process; Available Via Telnet/Ping. **Symptom:** User could not load firmware from FM while switch status unreachable. The switch was verified reachable via a telnet session and ping commands.
000025769	Medium	**Summary:** FM fails to timeout when it fails to receive a response to its http request sent to the switch. **Symptom:** User will encounter this problem only if the switch reboots or the webserver restarts on the switch during the time when Fabric Manager is waiting for a response to its' http request. **Workaround:** The cursor changes to an hour glass but Fabric Manager is still responsive. User can close and restart Fabric Manager to reset the cursor. **Customer Impact:** This is a stress test that is not likely to occur in a user SAN. There is a workaround and the application doesn't freeze. It can be fixed in a patch release. **Probability:** Low
000025953	Medium	**Summary:** 147675 FM Reports Different Times Stamps For Same Events Seen. **Symptom:** User may see a discrepancy between timestamps on the switch and the host.Solution: This works correctly because FM gets switch time in the event list response and adjusts all the event times to match the time relevant to the system time of the host machine it is running on, i.e. if the system time says 7:30 and the switch time says 6:30 and there was an event logged at 5:30, thru fabric manager the event time will says 6:30 as it will be adjusted by adding one hour due to the time difference between the switch time and the system time of the machine FM is running on. This correlates all the event times from different switches (with different) times to a time relevant to the user viewing them.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025954	Medium	**Summary:** 147553 Duplicate Switches Seen in SAN Elements. **Symptom:** This is due to an invalid wwn being given by the switch to FM during a fabric reconfiguration, the wwn is used in FM as a unique key and is not expected to be changing. This is a FOS defect and is being fixed. **Workaround:** Delete the fabric or fabrics and rediscover them.
000025955	Medium	**Summary:** 147550 Cannot Rename Switch Groups; Option Is Available. **Solution:** This works as expected as the ID display type wasn't of the type "name" for the tree and rename is only valid for the type "name". However this is confusing and in a future release we will disable the rename feature if the ID type displayed in the tree isn't of type "name".
000025115	Low	**Summary:** HBA Firmware Download returns 0(SUCCESS) even if the file sent is an invalid firmware or invalid file. **Symptom:** A customer could encounter this issue if they attempt to download a hba firmware version that is incompatible with the card they are using. **Workaround:** Ensure that the firmware that you are going to download to your hba is compatible with the card you are using.
000025957	Medium	**Summary:** Show/Hide Links -- Show Hide Node Canot Be Minimized or Resized; Blocking View. **Symptom:** When viewing a large Farbic, the legend box may be covering part of the view and would have to be moved to uncover that part. **Workaround**: Move the box around in the window as necessary. **Customer Impact:** Incovenience in not being able to minimize or turn off the legend. **Probability:** Will be an issue only when viewing large Fabrics or if the topology is zoomed in.

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025959	Medium	**Summary:** Topology View Does Not Indicate Which Switches Are Core Switches. **Symptom:** The topology vies does not readily indicate which switches are core switches except in core edge view where the core **switches are placed in the middle.** **Workaround:** Right click on a switch to see if core is checked on the menu which would indicate a core switch. **Customer Impact:** Inconvenience in not readily knowing which switches are core switches. **Probability:** Always
000025960	Medium	**Summary:** Topology View Shows The Switch For Entering Fabric When Clicking Open Space Near ISLs. **Symptom:** When clicking open space it shows the name of the Fabric or expanded node name. **Workaround:** Works as designed. Not a bug. Will investigate adding a prefix to indicate that it is a Fabric or a Group name. **Customer Impact:** None **Probability:** Always
000025961	Medium	**Summary:** Switches & ISLs Not Positioned Accurately After Changing Views. **Symptom:** Sometimes the links in the topology get confusing. **Workaround:** Click on link style icons to re-draw. **Customer Impact:** Topolgy view looks confusing when this issue occurs. **Probability:** Low

Table 1 Defects Open in Fabric Manager 4.0.1 (continued)

Defect ID	Severity	Summary
000025962	Medium	**Summary:** Topology Repositioned Each Time Bundles/ISL Selected. **Symptom:** When ISL bundles are expanded to provide optimal topolgy view of the Fabric some switches may be moved to a different position. **Workaround:** None **Customer Impact:** Inconvenience in not having the switches in the exact same location as before when ISL bundles are expanded. **Probability:** Depends on how optimal the layout is when links are expanded.
000025966	Low	**Summary:** Middle Mouse Button Used To Minimize Topology View; No Button To Expand. **Symptom:** Clicking middle mouse button would collapse the view. **Workaround:** Don't use middle mouse button. Use the expand and collapse icons on the topology view. **Customer Impact:** Since there is no mouse button to expand the view they would have to click on the + sign to expand the view. **Probability:** Since the documentation doesn't talk about using middle mouse button, it only happens if there is a middle mouse button and it is clicked by mistake.
000025967	Low	**Summary:** Topology View should default to Links Expanded. **Symptom:** The ISLs would all show as bundles or indivdulal links even if a bundle consists of a single link. **Workaround:** The bundles can all be expanded or collapsed as necessary. Works as designed. Not a bug. **Customer Impact:** User would have to expand the bundles to see individual links. **Probability:** Always

Defects Closed in Brocade Fabric Manager 4.0

Table 2 lists defects that have been closed in this release.

Table 2 Defects Closed in Brocade Fabric Manager 4.0

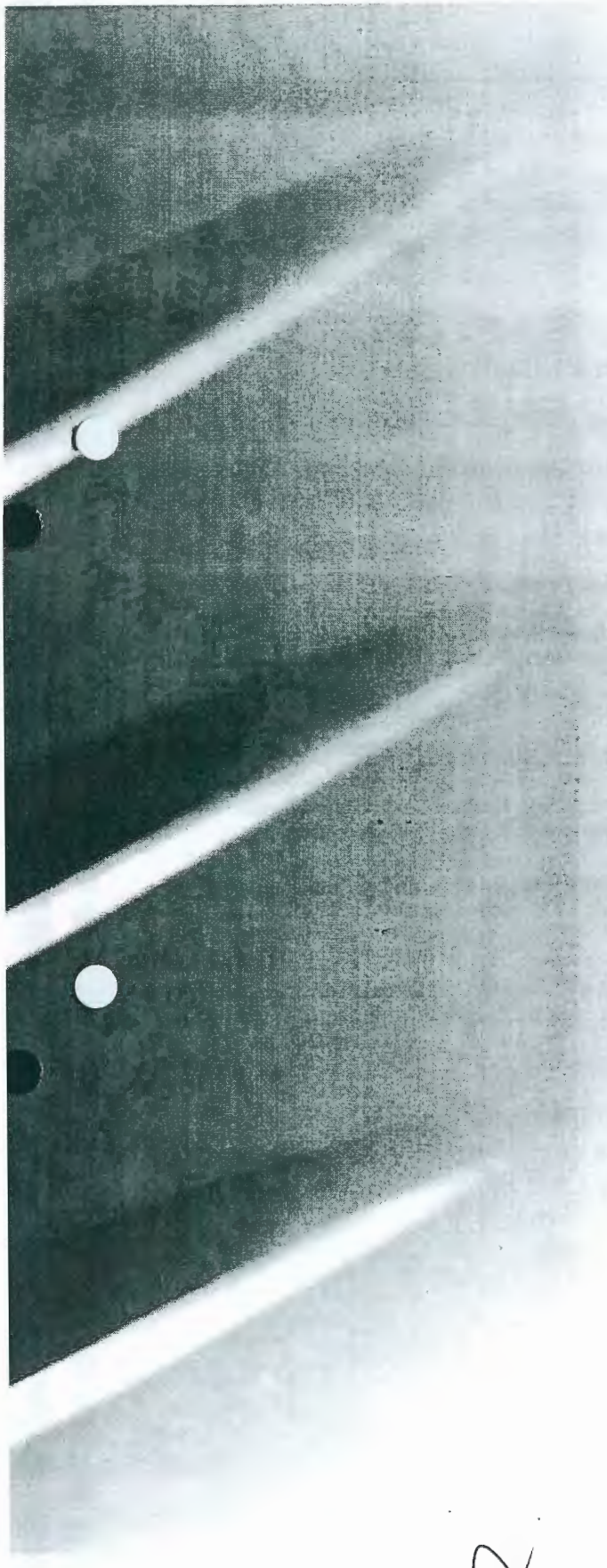
Defect ID	Severity	Summary
000025685	Medium	**Summary:** 143474 The Firmware Download/Firmware file: Path Should Not Require Full Path From root.
000025686	Medium	**Summary:** 143471 Deleted Item can reappear under switch group element.
000025716	Medium	**Summary:** 142983 EMC would like a reboot checkbox for sw2000 and sw3000.
000025724	Medium	**Summary:** Cannot establish a session in a multi-vendor fabricSymptom: In a multi-vendor fabric, using the Set Time, FDMI Refresh or HBA FirmwareDownload features within Fabric Manager, the operations.
000025789	Low	**Summary:** When Committing a Call Home config, for a lengthy commit, it is not readily apparent that the commit is still in progress.

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ECT
2303
Fls.
CPL - AC

ANEXO SWITCH TIPO 03
PARTE 3/A

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br



EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric OS

Version 4.1

REFERENCE MANUAL

P/N 300-000-637
REV A03

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B systems have been extensively tested and certified to meet UL1950, CSA 22.2 No 950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Preface

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric OS. Therefore, some functions described in this guide may not be supported by all versions of Fabric OS currently in use. For the most up-to-date information on product features, see the product release notes.

If an EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance.

Audience

This guide is part of the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B documentation set, and is intended for use by system administrators during installation and configuration of the DS-32B2 and ED-12000B switches.

Readers of this guide are expected to be familiar with the EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B operating environment

Organization

This manual provides the following information:

Chapter 1, *Telnet Commands* describes the various Telnet commands for EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B.

Chapter 2, *License Telnet Commands*, describes the commands that require a license key.

Chapter 3, *Fabric OS Version Comparison*, summarizes the commands available in v3.1 and v4.1.

Chapter 4, *Fabric and Switch Management*, explains the different methods used to manage a SAN for DS-32B2 and ED-12000B switches.

Chapter 5, *Control Processor Commands*, lists the commands available when logged into the Active CP and Standby CP in an ED-12000B.

Chapter 6, *Security and Commands*, summarizes the commands that are only available on the primary FCS when the security feature is enabled.

Chapter 7, *Supportshow Reference*, explains the information displayed by the `supportshow` command.

Appendix A, *Customer Support*, describes the procedure for contacting EMC Corporation when you need help with the EMC Connectrix Departmental Switch DS32B2 and Enterprise Director ED-12000B.

The *Glossary* defines terminology used in this manual.

Related Documentation

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Fabric Manager User Guide*
- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*

- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*

Conventions Used in this Guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

DANGER

A danger notice contains information essential to avoid a hazard that will cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical Conventions

EMC uses the following type style conventions in this guide:

Palatino, bold	◆ Dialog box, button, icon, and menu items in text ◆ Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	User entry. For example: **`symmpoll -p`**
AVANT GARDE	Keystrokes

Where to Get Help

Obtain technical support by calling your local sales office.

For service, call:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

and ask for Customer Support.

If you are located outside the USA, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

`http://www.emc.com/contact/`

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink Web site at:

http://powerlink.emc.com

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to techpub_comments@emc.com with your opinions of this guide.

1 Telnet Commands

This chapter describes the following commands:

agtcfgdefault

Reset the SNMP agent configuration to default values.

Syntax `agtcfgdefault`

Availability Admin

Description Use this command to reset the configuration of the SNMP agent to default values.

There is one SNMP agent per logical switch. This command is specific to the logical switch you are logged into.

Set the values for the following items:

- `sysDescr` — The system description. The default value is `Fibre Channel Switch`.
- `sysLocation` — The location of the system. The default value is `End User Premise`.
- `sysContact` — The contact information for the system. The default value is `Field Support`.
- `swEventTrapLevel` — The event trap level in conjunction with the event's severity level. When an event occurs and if its severity level is at or below the set value, the SNMP trap, swEventTrap, is sent to configured trap recipients. The default value is `0` (off), implying that no swEventTrap is sent. Possible values are:
  - 0 — none
  - 1 — critical
  - 2 — error
  - 3 — warning
  - 4 — informational
  - 5 — debug
- `authTraps` — When enabled, the authentication trap, authenticationFailure, is transmitted to a configured trap recipient in the event the agent received a protocol message that is not properly authenticated. In the context of SNMPv1 and SNMPv2c, this means that a request contains a community string that is not known to the agent. The default value for this parameter is 0 (disabled).

There are six communities and respective trap recipients supported by the agent. The first three communities are for read-write access (rw) and the last three are for read-only access (ro). Note that the factory default value for the trap recipient of each community is `0.0.0.0`. The factory default values for the community strings are:

```
Community 1: Secret Code
Community 2: OrigEquipMfr
Community 3: private
Community 4: public
Community 5: common
Community 6: FibreChannel
```

In order for an SNMP Management Station to receive a trap generated by the agent, the administrator must configure a trap recipient value to correspond to the IP address of the Management Station. In addition, the trap recipient must be able to pass the access control list (ACL) check.

The ACL check is as follows: There are six ACLs to restrict SNMP get/set operations to hosts under a host-subnet-area. Host-subnet-area is defined by comparing non-zero IP octets. For example, an ACL of `192.168.64.0` enables access for any hosts that start with `192.168.64`.xx. The connecting host is enabled to set each host-subnet-area to be read-write or read-only. Highest privilege matched out of six entries is given to the access. The ACL check is turned off when all six entries contain `0.0.0.0`.

When secure mode is enabled, the ACL feature is incorporated into the WSNMP and RSNMP security policies. Community strings can be changed on the primary FCS switch only and will propagate changes across the fabric.

Operands None

Example **To set the SNMP agent configuration parameters to the default values, and verify the default values are set:**

```
switch:admin> agtcfgdefault
*****
This command will reset the agent's configuration back to factory
   default
*****
Current SNMP Agent Configuration
Customizable MIB-II system variables:
           sysDescr = Fibre Channel Switch.
        sysLocation = End User Premise
         sysContact = Field Support.
```

```
  swEventTrapLevel = 0
  authTrapsEnabled = false

SNMPv1 community and trap recipient configuration:
  Community 1: Secret C0de (rw)
    No trap recipient configured yet
  Community 2: OrigEquipMfr (rw)
    No trap recipient configured yet
  Community 3: private (rw)
    No trap recipient configured yet
  Community 4: public (ro)
    No trap recipient configured yet
  Community 5: common (ro)
    No trap recipient configured yet
  Community 6: FibreChannel (ro)
    No trap recipient configured yet

SNMP access list configuration:
Entry 0:  No access host configured yet
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet

*****
Are you sure? (yes, y, no, n): [no] y
Committing configuration...done.
agent configuration reset to factory default
Current SNMP Agent Configuration
Customizable MIB-II system variables:
          sysDescr = Fibre Channel Switch
       sysLocation = End User Premise
        sysContact = Field Support
  swEventTrapLevel = 0
  authTrapsEnabled = false

SNMPv1 community and trap recipient configuration:
  Community 1: Secret Code (rw)
    No trap recipient configured yet
  Community 2: OrigEquipMfr (rw)
    No trap recipient configured yet
  Community 3: private (rw)
    No trap recipient configured yet
  Community 4: public (ro)
    No trap recipient configured yet
  Community 5: common (ro)
    No trap recipient configured yet
  Community 6: FibreChannel (ro)
    No trap recipient configured yet

SNMP access list configuration:
```

```
Entry 0:  No access host configured yet
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
switch:admin>
```

See Also
`agtcfgset`
`agtcfgshow`

agtcfgset

Modify the SNMP agent configuration.

Syntax `agtcfgset`

Availability Admin

Description Use this command to modify the configuration of the SNMP agent in the switch.

There is one SNMP agent per logical switch. This command is specific to the logical switch you are logged into.

Set the values for the following items:

- `sysDescr` — The system description. The default value is `Fibre Channel Switch`.
- `sysLocation` — The location of the system. The default value is `End User Premise`.
- `sysContact` — The contact information for the system. The default value is `Field Support`.
- `swEventTrapLevel` — The event trap level in conjunction with the event's severity level. When an event occurs and if its severity level is at or below the set value, the SNMP trap, swEventTrap, is sent to configured trap recipients. The default value is 0 (off), implying that no swEventTrap is sent. Possible values are:
  - 0 — none
  - 1 — critical
  - 2 — error
  - 3 — warning
  - 4 — informational

  - 5 — debug
- `authTraps` — When enabled, the authentication trap, authenticationFailure, is transmitted to a configured trap recipient in the event the agent received a protocol message that is not properly authenticated. In the context of SNMPv1 and SNMPv2c, this means that a request contains a community string that is not known to the agent. The default value for this parameter is 0 (disabled).

There are six communities and respective trap recipients supported by the agent. The first three communities are for read-write access (rw) and the last three are for read-only access (ro). Note that the factory default value for the trap recipient of each community is `0.0.0.0`. The factory default values for the community strings are:

```
Community 1: Secret Code
Community 2: OrigEquipMfr
Community 3: private
Community 4: public
Community 5: common
Community 6: FibreChannel
```

In order for an SNMP Management Station to receive a trap generated by the agent, the administrator must configure a trap recipient value to correspond to the IP address of the Management Station. In addition, the trap recipient must be able to pass the ACL check.

The ACL check is as follows: There are six ACLs to restrict SNMP get/set operations to hosts under a host-subnet-area. Host-subnet-area is defined by comparing non-zero IP octets. For example, an ACL of `192.168.64.0` enables access for any hosts that start with `192.168.64.xx`. The connecting host is enabled to set each host-subnet-area to be read-write or read-only. Highest privilege matched out of six entries is given to the access. The ACL check is turned off when all six entries contain `0.0.0.0`.

When secure mode is enabled, the ACL feature is incorporated into the WSNMP and RSNMP security policies. Community strings can be changed on the primary FCS switch only and will propagate changes across the fabric.

Operands None

Example To modify the SNMP configuration values:

```
switch:admin> agtcfgset
Customizing MIB-II system variables ...

At each prompt, do one of the following:
  o <Return> to accept current value,
  o enter the appropriate new value,
  o <Control-D> to skip the rest of configuration, or
  o <Control-C> to cancel any change.

To correct any input mistake:
<Backspace> erases the previous character,
<Control-U> erases the whole line,
sysDescr: [Fibre Channel Switch.]
sysLocation: [End User Premise]
sysContact: [Field Support.]
swEventTrapLevel: (0..5) [0]
authTrapsEnabled (true, t, false, f): [false]

SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address in dot notation: [0.0.0.0] 192.168.15.41
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (ro): [public]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (ro): [common]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address in dot notation: [0.0.0.0]

SNMP access list configuration:
Access host subnet area in dot notation: [0.0.0.0] 192.168.64.0
Read/Write? (true, t, false, f): [true] t
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
          sysDescr = Fibre Channel Switch.
       sysLocation = End User Premise
        sysContact = Field Support.
  swEventTrapLevel = 0
```

```
        authTraps = 0 (OFF)

SNMPv1 community and trap recipient configuration:
  Community 1: Secret C0de (rw)
    Trap recipient: 192.168.15.41
  Community 2: OrigEquipMfr (rw)
    No trap recipient configured yet
  Community 3: private (rw)
    No trap recipient configured yet
  Community 4: public (ro)
    No trap recipient configured yet
  Community 5: common (ro)
    No trap recipient configured yet
  Community 6: FibreChannel (ro)
    No trap recipient configured yet

SNMP access list configuration:
Entry 0:  Access host subnet area 192.168.64.0 (rw)]
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
Committing configuration...done.
switch:admin>
```

See Also `agtcfgdefault`
`agtcfgshow`

agtcfgshow

Display the SNMP agent configuration.

Syntax `agtcfgshow`

Availability All users

Description Use this command to display the configuration of the SNMP agent in the switch.

There is one SNMP agent per logical switch. This command is specific to the logical switch you are logged into.

Set the values for the following items:

- `sysDescr` — The system description. The default value is `Fibre Channel Switch`.

- `sysLocation` — The location of the system. The default value is `End User Premise`.
- `sysContact` — The contact information for the system. The default value is `Field Support`.
- `swEventTrapLevel` — The event trap level in conjunction with the event's severity level. When an event occurs and if its severity level is at or below the set value, the SNMP trap, swEventTrap, is sent to configured trap recipients. The default value is `0` (off), implying that no swEventTrap is sent. Possible values are:
  - 0 — none
  - 1 — critical
  - 2 — error
  - 3 — warning
  - 4 — informational
  - 5 — debug
- `authTraps` — When enabled the authentication trap, authenticationFailure, is transmitted to a configured trap recipient in the event the agent received a protocol message that is not properly authenticated. In the context of SNMPv1 and SNMPv2c, this means that a request contains a community string that is not known to the agent. The default value for this parameter is 0 (disabled).

There are six communities and respective trap recipients supported by the agent. The first three communities are for read-write access (rw) and the last three are for read-only access (ro). The factory default value for the trap recipient of each community is `0.0.0.0`. The factory default values for the community strings are:

```
Community 1: Secret Code
Community 2: OrigEquipMfr
Community 3: private
Community 4: public
Community 5: common
Community 6: FibreChannel
```

In order for an SNMP Management Station to receive a trap generated by the agent, the administrator must configure a trap recipient value to correspond to the IP address of the Management Station. In addition, the trap recipient must be able to pass the ACL check.

The ACL check is as follows: There are six ACLs to restrict SNMP get/set operations to hosts under a host-subnet-area.

Host-subnet-area is defined by comparing non-zero IP octets. For example, an ACL of 192.168.64.0 enables access for any hosts that start with 192.168.64.xx. The connecting host is enabled to set each host-subnet-area to be read-write or read-only. Highest privilege matched out of six entries is given to the access. The ACL check is turned off when all six entries contain 0.0.0.0.

When secure mode is enabled, the ACL feature is incorporated into the WSNMP and RSNMP security policies. Community strings can be changed on the primary FCS switch only and will propagate changes across the fabric.

Operands None

Example **To display SNMP agent configuration information:**

```
switch:admin> agtcfgshow
Current SNMP Agent Configuration
Customizable MIB-II system variables:
sysDescr = FC Switch
sysLocation = End User Premise
sysContact = Field Support.
swEventTrapLevel = 3
authTraps = 1 (ON)
SNMPv1 community and trap recipient configuration:
Community 1: Secret Code (rw)
Trap recipient: 192.168.1.51
Community 2: OrigEquipMfr (rw)
Trap recipient: 192.168.1.26
Community 3: private (rw)
No trap recipient configured yet
Community 4: public (ro)
No trap recipient configured yet
Community 5: common (ro)
No trap recipient configured yet
Community 6: FibreChannel (ro)
No trap recipient configured yet

SNMP access list configuration:
Entry 0:  Access host subnet area 192.168.64.0 (rw)]
Entry 1:  No access host configured yet
Entry 2:  No access host configured yet
Entry 3:  No access host configured yet
Entry 4:  No access host configured yet
Entry 5:  No access host configured yet
```

See Also `agtcfgdefault`
`agtcfgset`

aliadd

Add a member to a zone alias.

Syntax `aliadd "aliName", "member;member"`

Availability Admin

This command requires a zoning license.

Description Use this command to add one or more members to an existing zone alias. The alias member list cannot contain another zone alias.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

"aliName" Specify the name of a zone alias in quotation marks. This operand is required. A zone alias name must begin with a letter and can be followed by any number of letters, digits and underscore characters. Names are case sensitive, for example "Ali_1" and "ali_1" are different zone aliases. Blank spaces are ignored.

"member" Specify a member or list of members to be added to the alias, in quotation marks, separated by semi-colons. An alias member can be specified by one or more of the following methods:

- A switch domain and port area number pair. View the area numbers for ports using the switchshow command.
- WWN
- QuickLoop ALPAs

This operand is required.

Example **To add members to zone aliases array1, array2 and loop1:**

```
switch:admin> aliadd "array1", "1,2"
switch:admin> aliadd "array2", "21:00:00:20:37:0c:72:51"
switch:admin> aliadd "loop1", "0x02; 0xEF"
```

See Also

```
alicreate
alidelete
aliremove
alishow
```

alicreate

Create a zone alias.

Syntax `alicreate "aliName", "member;member"`

Availability Admin

This command requires a zoning license.

Description Use this command to create a new zone alias. The zone alias member list must have at least one member (empty lists are not allowed). The alias member list cannot contain another zone alias. Refer to the `zonecreate` command for more information on name and member specifications.

Zone Alias members can be specified using the Area number to represent a specific port and slot combination. Area numbers are automatically assigned to a port by the Fabric OS. You can view the Area numbers using the `switchshow` command.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

"aliName" Specify the name of a zone alias in quotation marks. This operand is required. A zone alias name must begin with a letter and can be followed by any number of letters, digits and underscore characters. Names are case sensitive, for example `"Ali_1"` and `"ali_1"` are different zone aliases. Blank spaces are ignored.

"member" Specify a member or list of members to be added to the alias, in quotation marks, separated by semi-colons. An alias member can be specified by one or more of the following methods:

- A switch domain and port area number pair. View the area numbers for ports using the `switchshow` command.
- WWN
- QuickLoop ALPAs

This operand is required.

Example **To create a zone alias:**

```
switch:admin> alicreate "array1", "2,32; 2,33; 2,34"
```

```
switch:admin> alicreate "array2", "21:00:00:20:37:0c:66:23"
switch:admin> alicreate "loop1", "0x02; 0xEF; 5,4"
```

See Also

```
aliadd
alidelete
aliremove
alishow
```

alidelete

Delete a zone alias.

Syntax `alidelete "aliName"`

Availability Admin

This command requires a zoning license.

Description Use this command to delete a zone alias.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operand:

"aliName"	Specify the name of zone alias to be deleted. This operand must be enclosed in quotation marks. This operand is required.

Example **To delete the zone alias array2:**

```
switch:admin> alidelete "array2"
```

See Also

```
aliadd
alicreate
aliremove
alishow
```

aliremove

Remove a member from a zone alias.

Syntax `aliremove "aliName", "member; member"`

Availability Admin

This command requires a zoning license.

Description Use this command to remove one or more members from an existing zone alias.

If all members are removed, the zone alias is deleted.

This command changes the defined configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

"aliName" Specify the name of the zone alias from which to have members removed in quotation marks. This operand is required.

"member" Specify a member or list of members to be removed from the alias, in quotation marks, separated by semicolons. An alias member can be specified by one or more of the following methods:

- A switch domain and port area number pair. View the area numbers for ports using the `switchShow` command.
- WWN
- QuickLoop AL_PAs

This operand is required. The member list is located by an exact string match; therefore, it is important to maintain the order when removing multiple members. For example, if a zone alias contains `"1,2; 1,3; 1,4"` then removing `"1,3; 1,4"` succeeds, but removing `"1,4; 1,3"` fails.

Example **To remove a member from array1:**

```
switch:admin> aliremove "array1", "3,5"
switch:admin> aliremove "array1", "21:00:00:20:37:0c:76:8c"
switch:admin> aliremove "array1", "0xEF"
```

See Also

```
aliadd
alicreate
alidelete
alishow
```

alishow

Display zone alias information.

Syntax `alishow "pattern", mode`

Availability All users

This command requires a zoning License.

Description Use this command to display zone configuration information.

If a parameter is specified, it is used as a pattern to match zone alias names; those that match in the defined configuration are displayed.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

"pattern"	A POSIX style regular expression used to match zone alias names. This operand must be enclosed in quotation marks. Patterns may contain: ◆ Question mark (?) that matches any single character. ◆ Asterisk (*) that matches any string of characters. ◆ Ranges that match any character within the range. Ranges must be enclosed in brackets, for example, [0-9] or [a-f]. This operand is optional.
mode	Specify `0` to display the contents of the transaction buffer (the contents of the current transaction), or specify `1` to display the contents of the non-volatile memory. The default value is `0`. This operand is optional.

If no parameters are specified, all zone configuration information (both defined and effective) is displayed. See `cfgshow` for a description of this display.

Example To show all zone aliases beginning with arr:

```
switch:admin> alishow "arr*"
alias: array1  21:00:00:20:37:0c:76:8c
alias: array2  21:00:00:20:37:0c:66:23
```

See Also

```
aliadd
alicreate
alidelete
aliremove
```

backplanetest

Run Backplane connection test for multiple blade configured system.

Syntax `backplanetest [-slot number] [-passcnt count] [-payload value] [-pat type] [-ports itemlist] [-verbose mode]`

Availability Admin

Description Use this command to verify the backplane connection of the blades through the back-end external ports. This command is for the ED-12000B only. This command assumes that all blades available on the specified switch have passed the blade diagnostic tests. This command is not part of the `bladediag` or `bladediagshort` commands. This command verifies backplane connection by using a functional blade's frame transmitter/receiver features.

When this test is running, no other diagnostic can be executed until this test is completed.

Operands This command has the following operands:

`-slot` *number*
: Specify the slot number for an ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

  The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

`-passcnt` *count*
: Specify the number of times to perform this test. The default value is `1`. This operand is optional.

`-payload` *value*
: Specify the byte size of the test frame payload. The payload size must be in multiples of 4 and the minimum size is 16. The default value is 512 bytes. This operand is optional.

`-pat type` — Specify the test pattern type used in the test frame payload. The default test is 17(jCRPAT). The following test patterns can be specified:

- 1 byte fill
- 2 word fill
- 3 quad fill
- 4 byte not
- 5 word not
- 6 quad not
- 7 byte ramp
- 8 word ramp
- 9 quad ramp
- 10 byte lfsr
- 11 random
- 12 crpat
- 13 cspat
- 14 chalf sq
- 15 cqtr sq
- 16 rdram pat
- 17 jCRPAT (default)
- 18 jCJTPAT
- 19 jCSPAT

`-ports itemlist` — Specify a list of blade ports to test. By default, all the blade ports in the specified slot are used. See `itemlist` for further details.

`-verbose mode` — Specify the verbose mode. If specified with non- zero value, it will display the test progress in detail. The default value is to disable the mode. This operand is optional.

Example **To run a backplane connection test on an ED-12000B switch:**

```
switch:admin> backplanetest -ports 1/16, 18, 20 -payload 2048 -verbose 1
Running backplanetest ..............

Test frame info for Backplane Connection Test:
# of frames:  1
sid data:     0xfffffd
did data:     0xfffffd
payload size: 2048 bytes
```

```
Test Complete: backplanetest Pass 1 of 1
Duration 0 hr, 0 min & 1 sec (0:0:1:715).
 passed.

switch:admin>
```

Errors When this command detects failure(s), the subtest may report one or more of the following error messages:

```
DATA
TIMEOUT
XMIT
```

See Also

```
itemlist
bladediag
bladediagshort
```

backport

Run test for back-end ASIC to ASIC links.

Syntax `backport [-nframes` *`count`*`] [-ports` *`itemlist`*`] [-lb_mode` *`mode`*`] [-fr_type` *`type`*`] [-extonly` *`mode`*`]`

Availability Admin

Description Use this command to test the backplane routing and virtual channel (VC) allocation. This test applies to single blade as well as multi-blade systems.

The following items are tested:

- Proper back-end port domain routing setup such that every user port has a valid path to every other user port. If a valid path does not exist between any two user ports then that path will fail to transmit the first frame between the two ports.
- Proper VC mapping such that an arbitrarily large number of frames may be transmitted without running out of credit. If the VC credit mapping is not correct, then the test will fail after enough frames have been sent to exhaust the initial credit. VC mapping is not tested if the `extonly` operand is enabled.
- Proper trunking of backend ports. The frames are sent in bursts. If the trunking is not set up properly, the burst of frames will not arrive in order.

Since the frames are received without *spinning* first, this test is not as exhaustive as `spinfab`.

- ASIC errors along each path. The test will check for CRC and ENC errors for each port used between the source and destination ports to help isolate failures. It will also check that each member of every trunk group along the path has sent or received at least one frame.

Operands This command has the following operands:

`-nframes` *`count`* Specify the number of frames per port to send. The test runs until the specified number of frames have been transmitted on each port. The total number of frames that this command circulates is determined at run time. The default value is `10` and the minimum value is `3`. Any value less than the minimum is ignored and the minimum value is used.

`-ports` *`itemlist`* Specify a list of user ports. The default value is all user ports. Refer to `itemlist` for more information.

`-lb_mode` *`mode`* Select the loopback point for the test. By default, backport uses internal loopback.

Mode	Description
1	Port Loopback (loopback plugs)
2	External (SERDES) loopback
5	Internal (parallel) loopback

`-fr_type` *`type`* Specify the frame type to send. The default type is `1`. The valid types are:

Type	Description
0	single frame
1	spinfab frames
2	spinfab 1K frames

`-extonly` *mode*

Specify the external test only mode. The default value is 0 which disables the external test only mode. This command normally sends bursts of frames from each port under test to every other port in the list. With `-extonly` mode set to `1`, the command sends only one burst of frames to each port from each ASIC pair to ASIC pair link. This tests all of the external connections with only K * N frames instead of the N^2 frames required in the all to all mode.

This mode is intended to be used in ESS/Burnin testing to optimize test time. `backport` tests only the external connections between each ASIC pair. `txdpath` is used to test the internal ASIC pair to ASIC pair paths.

Valid values are:

- 0 Send frames from all ports to all other ports.
- 1 Send only one burst of frames to each link.

Example **To test for back-end ASIC pair links:**

```
switch:admin> backport -ports 1/1-1/3 -nframes 10
One moment please ...
backport running...
backport: Completed 840 frames, status:  passed.
switch:admin>
```

Errors When the command detects failure(s), the test may report one or more of the following error messages:

```
ERR_STAT
ERR_STATS
INIT
PORT_DIED
PORT_STOPPED
XMIT
```

See Also

```
crossporttest
itemlist
portloopbacktest
spinfab
spinsilk
txdpath
```

bannerset

Set the banner on the local switch.

Syntax `bannerset [banner]`

Availability Admin

Description Use this command to set the banner on the local switch.

The banner is a string of alphanumeric characters. It is displayed whenever a user tries to log into a switch.

The banner can be created using the banner operand or by entering the `bannerset` command without an operand, making the session interactive.

If you enter the banner text using the interactive method, the valid length is 1022 characters. If the banner text length exceeds the maximum allowed, the software truncates the input. To close thebanner text string, enter a period at the beginning of a new line.

Operands This command has the following operand:

banner	Specify a text string to be displayed when a user logs in. If you enter the banner text using the banner operand, the valid length is only 116 characters. This operand is optional.

Example **To set a new banner for a switch:**

```
switch:admin> bannerset "My banner"

switch:admin> bannerSet
Please input context of security banner (press "." RETURN
   at the
beginning of a newline to finish input): Do not log into
   this
switch if you are not an authorized administrator.
.
switch:admin>
```

See Also bannershow

bannershow

Display the banner text.

Syntax bannershow

Availability Admin

Description Use this command to display the contents of the banner.

Operands None

Example **To display the banner for a switch:**

```
switch:admin> bannershow
Banner:
Do not log into this switch if you are not an authorized
   administrator.
switch:admin>
```

See Also bannerset

bcastshow

Display broadcast routing information.

Syntax `bcastshow`

Availability All users

Description Use this command to display the broadcast routing information for all ports in the switch. The broadcast routing information indicates all ports that are members of the broadcast distribution tree that is, ports that are able to send and receive broadcast frames.

Normally, all F_Ports and FL_Ports are members of the broadcast distribution tree. The broadcast path selection protocol selects the E_Ports that are part of the broadcast distribution tree. The E_Ports are chosen in such a way to prevent broadcast routing loops.

The following fields are displayed:

`Group`	The multicast group ID of the broadcast group.
`Member Ports`	A map of all ports in broadcast tree.
`Member ISL Ports`	A map of all E_Ports in broadcast tree.
`Static ISL Ports`	Reserved.

The broadcast routing information for the ports is displayed as a set of hexadecimal bit maps. For more information on reading hexadecimal bitmaps, refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric OS Procedures Manual*.

The output from this command varies depending on switch type.

Operands None

Examples **To display the broadcast routing information for all ports in the switch:**

```
switch:admin> bcastshow
Group   Member Ports    Member ISL Ports        Static ISL Ports
--------------------------------------------------------------------
 256     0x82000000        0x02000000              0x00000000
```

```
          0x00180000        0x00100000              0x00000000
          0x00000001        0x00000000              0x00000000
switch:admin>
```

See Also `mcastshow`
`portrouteshow`

bladebeacon

Set blade beaconing mode on or off.

Syntax `bladebeacon [slotnumber] mode`

Availability Admin

This command is only available on the ED-12000B switch.

Description Use this command to set the blade beaconing mode on or off. Specify mode `1` to enable beaconing mode, or specify mode `0` to disable beaconing.

When beaconing mode is enabled, the port LEDs will flash amber in a running pattern from port 0 through port 15 and back again. The pattern continues until the user turns it off. This can be used to locate a physical unit.

Beaconing mode only takes over the port LEDs, it does not change the switch's functional behavior. The normal flashing LED pattern (associated with an active, faulty, or disabled port for example) is suppressed and only the beaconing pattern is displayed. If a diagnostic frame-based test (such as `portloopbacktest`, `crossporttest`, or `spinsilk`) is executed, the two LED patterns are interwoven. The diagnostic test flickers the LEDs green and the beaconing mode runs the LEDs amber.

The `switchshow` command can be used to display if the status of blade beaconing mode is on or off.

Operands This command has the following operands:

slotnumber	Specify the slot number to enable bladebeacon.
mode	Specify a value of 1 to set beaconing mode On. Specify a value of 0 to set beaconing mode Off. This operand is required.

Example **To turn the blade in slot 2 beaconing mode On and then Off:**

```
switch:admin> bladebeacon 2 1
switch:admin> bladebeacon 2 0
```

See Also `switchshow`

bladediag

Run diagnostics on a switch blade.

Syntax `bladediag [[-slot] number][-log logfile]`

Availability Admin

Description Use this command to run a suite of diagnostics tests on the specified switch blade (modular products only). To run this command you must install loopback plugs on every port. (Run `systemtest` otherwise.) The tests executed are:

- `portregtest`
- `centralmemorytest`
- `cmitest`
- `camtest`
- `filtertest`
- `statstest`
- `portloopbacktest`
- `txdpath`
- `crossporttest`
- `turboramtest`
- `spinsilk`
- `backport`
- `diagshow`

Compared to `bladediagshort`, this is a comprehensive test for blade functionality which also involves backplane connections

Each diagnostic test in this suite may report its own set of error messages when it detects failures. See the *Errors* section of each of the individual commands listed in this chapter.

Operand This command has the following operands:

`-slot` *number* — Specify the slot number of the blade on which you want to run diagnostics. This operand is for a modular switch only and is optional. For all other switches this operand is not required.

`-log` *logfile* — Specify that the output of the command will be placed in a file named by the `logfile` argument. The log file will contain all activity that occurred during the execution of the command. All error messages are also saved in the logfile. If this option is not specified, no log file is created.

Example **To run a suite of diagnostics on blade3:**

```
switch:admin> bladediag --slot 3
Testing user ports: 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

turboramtest

Running turboramtest ..............
Test Complete: turboramtest Pass 1 of 1
Duration 0 hr, 0 min & 6 sec (0:0:6:635).
 passed.

portregtest

Running portregtest ..............
Test Complete: portregtest Pass 1 of 1
Duration 0 hr, 2 min & 20 sec (0:2:20:986).
 passed.

centralmemorytest

Running centralmemorytest ..............
Test Complete: centralmemorytest Pass 1 of 1
Duration 0 hr, 0 min & 19 sec (0:0:19:767).
 passed.
--- <output truncated> ---
```

See Also `backport`
`bladediagshort`


```
switchdiag
switchdiagshort
camtest
centralmemorytest
cmitest
crossporttest
diagshow
filtertest
portloopbacktest
portregtest
spinsilk
statstest
systemtest
turboramtest
txdpath
```

bladediagshort

Run diagnostics on a switch blade.

Syntax `bladediagshort [[-slot] number][-log logfile]`

Availability Admin

Description Use this command to run a suite of diagnostics tests on the specified switch blade (modular products only). To run this command you must install loopback plugs on every port. (Run `systemtest` otherwise.) The tests executed are:

- `portregtest`
- `centralmemorytest`
- `cmitest`
- `camtest`
- `filtertest`
- `statstest`
- `portloopbacktest`
- `txdpath`
- `crossporttest`
- `turboramtest`
- `spinsilk`
- `backport`
- `diagshow`

Compared to `bladediag`, this is a limited test for single blade functionality, which does not involve backplane connections.

Each diagnostic test in this suite may report its own set of error messages when it detects failures. See the *Errors* section of each of the individual commands listed in this chapter.

Operands This command has the following operands:

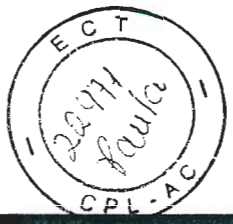
`-slot` *number*	Specify the slot number of the blade on which you want to run diagnostics. This operand is for a modular switch only and is optional. For all other switches this operand is not required.
`-log` *logfile*	Specify that the output of the command will be placed in a file named by the `logfile` argument. The log file will contain all activity that occurred during the execution of the command. All error messages are also saved in the logfile. If this option is not specified, no log file is created.

Example **To run a suite of diagnostics on blade 3:**

```
switch:admin> bladediagshort --slot 3
Testing user ports: 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

turboramtest

Running turboramtest ..............
Test Complete: turboramtest Pass 1 of 1
Duration 0 hr, 1 min & 47 sec (0:1:47:181).
 passed.

portregtest

Running portregtest ..............
Test Complete: portregtest Pass 1 of 1
Duration 0 hr, 2 min & 21 sec (0:2:21:698).
 passed.
--- <output truncated> ---
```

See Also

- backport
- bladediag
- switchdiag
- switchdiagshort
- camtest
- centralmemorytest
- cmitest
- crossporttest
- diagshow




```
filtertest
portloopbacktest
portregtest
spinsilk
statstest
systemtest
turboramtest
txdpath
```

bladedisable

Disable a blade.

Syntax `bladedisable [slotnumber]`

Availability Admin

Description Use this command to disable a blade. All Fibre Channel ports are taken offline. If the switch was connected to a fabric through this blade, the remaining switches reconfigure, and this switch will configure based on the other blade ports.

The blade must be disabled before making configuration changes or before running many of the diagnostic tests.

The blade does not need to be disabled before rebooting or powering off.

The disable process may be observed and verified by watching the front panel LEDs change to slow flashing yellow as each port of the blade is disabled.

A blade cannot be disabled or enabled when the switch is disabled.

Operands This command has the following operand:

slotnumber	Specify the slot number to be disabled.

Example **To disable a blade in slot 2:**

```
switch:admin> bladedisable 2
```

See Also

```
switchshow
bladeenable
portenable
portdisable
```

bladeenable

Enable a blade.

Syntax `bladeenable [slotnumber]`

Availability Admin

Description Use this command to enable a blade. All Fibre Channel ports within the blade which did not fail POST are enabled, and may come online if connected to a device, or remain offline if disconnected. The switch may need to be enabled if it was previously disabled to make configuration changes or to run diagnostics.

If the switch is connected to a fabric, it rejoins the fabric. After this command is issued, the 10 second fabric stability count down is displayed. If this switch remains the principal switch at the end of the count down, then it assigns itself a domain ID. If another switch assumes the principal role, then this switch becomes a subordinate switch, and accepts a domain ID from the principal.

The enable process may be observed and verified by watching the front panel LEDs change from slow flashing yellow as each port is enabled. The LEDs change to green for online ports, or may remain black for disconnected ports, or yellow for ports that do not initialize.

A blade cannot be disabled or enabled when the switch is disabled.

Operands This command has the following operand:

slotnumber	Specify the slot number to be enabled.

Example **To enable a blade in slot 2:**

```
switch:admin> bladedisable 2
```

See Also

```
switchshow
bladedisable
portdisable
portenable
```

bladepropshow

Display blade property.

Syntax `bladepropshow [[-slot] number]`

Availability All users

Description Use this command to display the properties of a blade.

The output of this command is intended for support use only.

Operands This command has the following operand:

`-slot number`	Specify the slot number of the blade you which you want to run diagnostics. The default is set to `0` and designed to operate on fixed port count products. This operand is optional.

Example **To display the blade properties for blade 7:**

```
switch:admin> bladepropshow -slot 7

   Slot: 7
   [2,4/8/64]
   <0,1657/0001 1,1657/0001>
   <2,1657/0001 3,1657/0001>
   <4,1657/0001 5,1657/0001>
   <6,1657/0001 7,1657/0001>
   <0,8>=<1,9> <0,10>=<2,9> <0,6>=<3,7>
   <1,9>=<0,8> <1,6>=<2,7> <1,10>=<3,9>
   <2,9>=<0,10> <2,7>=<1,6> <2,10>=<3,11>
   <3,7>=<0,6> <3,9>=<1,10> <3,11>=<2,10>
```

See Also `chippropshow`
`ptpropshow`

camtest

Tests the functionality of Content Addressable Memory (CAM).

Syntax `camtest [-slot number][-passcnt count][-txport itemlist]`

Availability Admin

Description Use this command to verify that Content Addressable Memory (CAM) is functionally correct. The CAM is used by QuickLoop to translate the SID.

When a CAM is presented with a data, it checks if the data is present in its memory. A hit means the data is found in the CAM. A miss means the data is not found.

In this test, the CAM is filled with four kinds of data patterns:

1. A walking 1,
2. A walking 0,
3. A random pattern,
4. An inverted version of the random pattern above.

Once filled with each of the patterns above, a frame is sent and looped back internally. If a hit is expected (when the random or inverted random pattern is used) the original SID in the frame transmitted is received translated with the domain and area fields of the SID zeroed. If a miss is expected (when the walking 1 or walking 0 pattern is used) the original SID in the frame transmitted is received unchanged.

This command may not be executed on an enabled switch. You must first disable the switch using the `switchdisable` command.

Operands This command has the following operands:

`-slot` *number*	Specify the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is set to `0` and designed to operate on fixed port count products.
`-passcnt` *count*	Specify the number of times to execute this test. The default value is `1`.
`-txport` *list*	Specify a list of blade ports to test. By default, all the blade ports in the specified slot (`-slot`) will be used. See `itemlist` for more information.

Example **To verify that Content Addressable Memory (CAM) is functioning correctly:**

```
switch:admin> camtest -txports 1/1
Running camtest ..............
Test Complete: "camtest" Pass 1 of 1
Duration 0 hr, 0 min & 5 sec (0:0:5:14).
 passed.
```

Errors Below are possible error messages if failures are detected:

```
DIAG-CAMFLTR
DIAG-CAMINIT
DIAG-CAMSID
DIAG-CAMSTAT
DIAG-CANTXMIT
```

See Also

```
centralmemorytest
cmemretentiontest
cmitest
crossporttest
itemlist
portloopbacktest
portregtest
spinsilk
sramretentiontest
```

centralmemorytest

Perform a bit write/read test of the ASIC central memory.

Syntax

```
centralmemorytest [-slot number] [-passcnt
   count] [-datatype type] [-ports itemlist] [-seed value]
```

Availability

Admin

Description

Use this command to verify the address and data bus of the ASIC SRAMs that serve as the central memory.

This command may not be executed on an enabled switch. You must first disable the switch using the `switchdisable` command.

The test consists of six subtests:

Subtest 1

The BISR subtest executes the Built-In-Self-Repair (BISR) circuitry in each ASIC. The BISR executes its own BIST, and cells found bad are replaced by redundant rows provided in each SRAM in the ASIC. Once replaced, the BIST is executed again.

The firmware merely sets up the hardware for the BISR/BIST operation and checks the results. If the done bit in each SRAM is not set within a time-out period, it reports the DIAG-CMBISRTO. If any of the SRAMs within the ASIC fails to map out the bad rows, its fail bit is set and the DIAG-CMBISRF error generated.

Subtest 2

The data write/read subtest executes the address and data bus verifications by running a specified unique ramp pattern D to all SRAMs in all ASICs in the switch. When all SRAMs are written with pattern D, the SRAMs are read and compared against the data previously written. The above step is repeated with the complemented pattern ~D to ensure that each data bit is toggled during the test.

The default pattern used (by POST also) is a QUAD_RAMP with a seed value of 0.

Subtest 3

The ASIC-to-ASIC connection subtest verifies that any port can read the data from any of the ASICs in the switch; thus verifying both the

logic transmitting and receiving the data and the physical transmit data paths on the main board connecting all the ASICs to each other.

Subtest 3 is not available on 2 Gbits/sec capable switches.

The test method is as follows:

1. Fill the Central Memory of all ASICs with unique frames.
2. Set up the hardware such that each ASIC is read by all of the MAX number of ports in the switch. Data received is compared against the frame written into the ASIC.
   - Port 0 reads the Central Memory in ASIC 0
   - Port 1 reads the Central Memory in ASIC 0
   - Port 14 reads the Central Memory in ASIC 0
   - Port 15 reads the Central Memory in ASIC 0
   - Port 0 reads the Central Memory in ASIC 1
   - Port 1 reads the Central Memory in ASIC 1
   - Port 14 reads the Central Memory in ASIC 1
   - Port 15 reads the Central Memory in ASIC 1
   - Port 15 reads the Central Memory in ASIC 2
   - Port 15 reads the Central Memory in ASIC 3
3. Repeat the steps above for the complemented pattern.
4. Repeat for each mini-switch in the blade under test

The pattern used is generated similarly as in subtest 2 above except that only 2112 bytes are generated.

Subtest 4

The forced bad parity error subtest verifies that a bad parity can be detected, its error flag set, and an interrupt bits are set

The test method is as follows:

1. Clear the error and interrupt bits of all ASICs
2. Write 64 bytes with bad parity to all ASICs at offset 0
3. Read each of the ASICs at offset 0 & check that the error and interrupt bits are set.
4. Repeat the steps above for offset 1, 2, 3, ... 10

Subtest 5

The forced bad buffer number error subtest verifies that the bad buffer number in the data packet can be detected, its error flag and interrupt bits are set.

The test method is as follows:

1. Clear the error and interrupt bits of all ASICs.
2. Set up the hardware so that transmission of data includes a bad buffer number.
3. For each ASIC X in the switch, do:
   For each of the 11 possible offsets, do:
   a. Write a 64 byte pattern in the Central Memory.
   b. Read X from all ASIC Y in the switch.
   c. Check that X has its:
      - interrupt bits are set.
      - error type is buffer number error.
      - the port number in error is the receiver port (which is the base port of ASIC Y).
4. Check that all other ASICs (~X) *do not* get:
   - an interrupt, or
   - an error flagged.
5. Reading the error register clears the CMEM interrupt bit; ready for the next offset to test.

Subtest 6

The forced bad chip number error subtest verifies that the bad buffer number in the data packet can be detected, its error flag and interrupt bits are set.

The test method is as follows:

1. Clear the error and interrupt bits of all ASICs.
2. Set up the hardware so that transmission of data includes a bad buffer number.
3. For each ASIC X in the switch, do:
   For each of the 11 possible offsets, do:
   a. Write a 64 byte pattern in the Central Memory.
   b. Read X from all ASIC Y in the switch.

c. Check that all ASIC Y has its:
   - interrupt bits are set.
   - error type is chip number error.
   - the port number in error is the receiver port (which is the base port of asic Y).

d. Reading the error register clears the CMEM interrupt bit; ready for the next offset to test.

Operands This command has the following operands.-

`-slot` *number* — Specify the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is set to `0` and designed to operate on fixed port count products.

`-passcnt` *count* — Specify the number of test passes to run. By default the test will be run one time.

`-datatype` *type* — Specify the type of data pattern to use. By default, type 9, QUAD_RAMP is used. For a complete list of supported data patterns run the `datatypeshow` command. Some common settings are:

- 1 BYTE_FILL pattern.
- 2 WORD_FILL pattern.
- 3 QUAD_FILL pattern.
- 9 QUAD_RAMP (Addr=Data) pattern.
- 11 RANDOM pattern.

`-ports` *itemlist* — Specify a set of ports to test. Specify a list of blade ports to test. The Ports list is translated into a matching quad list before the test is run. By default all the blade ports in the specified slot (`-slot`) are tested. See `itemlist` for more information.

`-seed` *value* — Specify the data pattern seed to be used. The default seed value is `0`.

Example **To test the ASIC central memory:**

```
switch:admin> centralmemorytest -ports 1/0-1/15
Running centralmemorytest ............
Test Complete: "centralmemorytest" Pass 1 of 1
Duration 0 hr, 0 min & 5 sec (0:0:5:412).
passed.
```

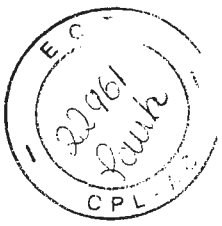
Errors

When this command detects failure(s), each subtest may report one or more of the following error messages:

```
Subtest 2
    LCMEM_ERR
    LCMRS_ERR
    LCMTO_ERR
Subtest 3
    CM_NO_BUF
    LCMEMTX_ERR
    LCMRS_ERR
    LCMTO_ERR
Subtest 4
    BAD_INT
    CM_ERR_PTN
    CM_ERR_TYPE
    TIMEOUT
Subtest 5
    BAD_INT
    CM_ERR_PTN
    CM_ERR_TYPE
    TIMEOUT
Subtest 6
    BAD_INT
    CM_ERR_PTN
    CM_ERR_TYPE
    TIMEOUT
```

See Also

```
camtest
cmemretentiontest
cmitest
crossporttest
itemlist
portloopbacktest
portregtest
spinsilk
sramretentiontest
```



cfgactvshow

Display Effective zone configuration information.

Syntax `cfgactvshow`

Availability All users

This command requires a zoning license.

Description Use this command to display the Effective zone configuration information.

The Effective configuration is a single zone configuration that is currently in effect. The devices that an initiator sees are based on this configuration. The Effective configuration is built when a specified zone configuration is enabled.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To show the Effective zone configuration information:**

```
switch:admin> cfgactvshow
Effective configuration:
cfg:   c4
zone:  z3       33:07:06:05:04:03:02:01
zone:  z4       44:01:23:45:67:89:a0:bc
switch:admin>
```

See Also

```
cfgclear
cfgcreate
cfgdelete
cfgremove
cfgsave
cfgshow
```

cfgadd

Add a member to a zone configuration.

Syntax `cfgadd "cfgName", "member; member"`

Availability Admin

This command requires a zoning license.

Description Use this command to add one or more members to an existing zone configuration.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

cfgName	Specify a name for the zone configuration in quotation marks. This operand is required.
member	Specify a member or list of members to be added to zone configuration, in quotation marks, separated by semicolons. Members can be specified in one or more of the following methods: ◆ Zone names ◆ QuickLoop names ◆ FA (Fabric Assist) zone names This operand is required.

Example **To add new zones to the configuration "Test_cfg":**

```
switch:admin> cfgadd "Test_cfg", "redzone; bluezone"
```

See Also

```
cfgclear
cfgcreate
cfgdelete
cfgdisable
```

```
cfgenable
cfgremove
cfgsave
cfgshow
cfgtransabort
cfgtransshow
```

cfgclear

Clear all zone configurations.

Syntax `cfgclear`

Availability Admin

This command requires a zoning license.

Description This command clears all zone information in the transaction buffer. All defined zone objects in the transaction buffer are deleted. If you attempt to commit the empty transaction buffer while a zone configuration is enabled, a warning displays, to first disable the enabled zone configuration or to provide a valid configuration with the same name.

After clearing the transaction buffer using the `cfgclear` command, use the `cfgdisable` command to commit the transaction, and disable and clear the zone configuration in non-volatile memory for all the switches in the fabric.

If no effective zoning configuration exists, then use the `cfgsave` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To clear all zones, and then clear nonvolatile memory:**

```
switch:admin> cfgclear
   Do you really want to clear all configurations?
   (Yes, y, no, n): [no] yes
   switch:admin> cfgsave
```

See Also `cfgadd`

```
cfgcreate
cfgdelete
cfgdisable
cfgenable
cfgremove
cfgsave
cfgshow
cfgtransabort
cfgtransshow
```

cfgcreate

Create a zone configuration.

Syntax `cfgcreate "cfgName", "member; member"`

Availability Admin

This command requires a zoning license.

Description Use this command to create a new zone configuration.

A zone configuration name must begin with a letter and can be followed by any number of letters, digits, and underscore characters. Names are case-sensitive, for example `Cfg_1` and `cfg_1` are different zone configurations. Blank spaces are ignored.

The zone configuration member list must have at least one member (empty lists are not allowed).

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

Refer to the `zonecreate` command for more information on name and member specifications.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

cfgName Specify a name for the zone configuration in quotation marks. This operand is required.

member Specify a member or list of members to be added to zone configuration, in quotation marks, separated by semicolons.

Members can be specified in one or more of the following methods:

- Zone names
- QuickLoop name
- FA (Fabric Asssit) zone names

This operand is required.

Example **To create a configuration containing three zones:**

```
switch:admin> cfgcreate "Test_cfg", "redzone; bluezone;
   greenzone"
```

See Also

```
cfgadd
cfgclear
cfgdelete
cfgdisable
cfgenable
cfgremove
cfgsave
cfgshow
cfgtransabort
cfgtransshow
```

cfgdelete

Delete a zone configuration.

Syntax `cfgdelete "cfgName"`

Availability Admin

This command requires a zoning license.

Description Use this command to delete a zone configuration.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile

memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operand

This command has the following operand:

cfgName	Specify the name of zone configuration to be deleted in quotation marks. This operand is required.

Example

To delete a zone configuration:

```
switch:admin> cfgdelete "Test_cfg"
```

See Also

`cfgadd`
`cfgclear`
`cfgcreate`
`cfgdisable`
`cfgenable`
`cfgremove`
`cfgsave`
`cfgshow`
`cfgtransabort`
`cfgtransshow`

cfgdisable

Disables an effective zone configuration.

Syntax

`cfgdisable`

Availability

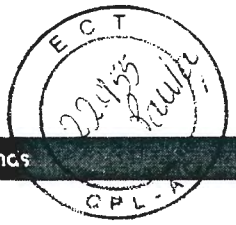
Admin

This command requires a zoning license.

Description

Use this command to disable the current zone configuration. The fabric returns to nonzoning mode where all devices see each other.

This command ends and commits the zone configuration in the transaction buffer to volatile and nonvolatile memory. If a transaction is open on a different switch in the fabric when this command is run,



the transaction on the other switch is automatically aborted. A message is displayed on the other switches to indicate the aborting of the transaction.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To disable the current zone configuration:**

```
switch:admin> cfgdisable
Updating flash ...
switch:admin>
```

See Also

```
cfgadd
cfgclear
cfgcreate
cfgdelete
cfgenable
cfgremove
cfgsave
cfgshow
cfgtransabort
cfgtransshow
```

cfgenable

Enables a zone configuration.

Syntax `cfgenable "cfgName"`

Availability Admin

This command requires a zoning license.

Description This command commits the zone configuration in the transaction buffer to the volatile and nonvolatile memory and enables the specified zone configuration. This command ends the current zoning transaction.

The specified zone configuration is built by checking for undefined zone names, zone alias names, or other inconsistencies; by expanding zone aliases, removing duplicate entries, and then installing the effective configuration.

If the build fails, the previous state is preserved (zoning remains disabled, or the previous effective configuration remains in effect). If the build succeeds, the new configuration replaces the previous configuration. Refer to the `cfgshow` command for a description of defined and effective configurations.

This command ends and commits the current transaction. If a transaction is open on a different switch in the fabric when this command is run, the transaction on the other switch is automatically aborted. A message is displayed on the other switches to indicate the aborting of the transaction.

When security is enabled, this command can only be issued from the primary FCS switch.

Operand

This command has the following operand:

cfgName	Specify the name of a zone configuration in quotation marks. This operand is required.

Example

To enable the zone configuration Test_cfg:

```
switch:admin> cfgenable "Test_cfg"
zone config "Test_cfg" is in effect
```

See Also

`cfgadd`
`cfgclear`
`cfgcreate`
`cfgdelete`
`cfgdisable`
`cfgremove`
`cfgsave`
`cfgshow`
`cfgtransabort`
`cfgtransshow`

cfgremove

Remove a member from a zone configuration.

Syntax `cfgremove "cfgName", "member; member"`

Availability Admin

This command requires a zoning license.

Description Use this command to remove a member from an existing zone configuration.

The member list is located by an exact string match, therefore, it is important to maintain the order when removing multiple members. For example, if a zone configuration contains `zone2; zone3; zone4` then removing `zone3; zone4` succeeds, but removing `zone4; zone3` fails.

If all members are removed, the zone configuration is deleted.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands The following operands are required:

"cfgName"	Specify a name of a zone configuration, in quotation marks.
"member"	Specify a member or list of members to be deleted from the zone configuration, in quotation marks, separated by semicolons. Members can be specified in one or more of the following methods: ◆ Zone names ◆ QuickLoop names ◆ FA (Fabric Assist) zone names This operand is required.

Example **To remove a zone from a configuration:**

```
switch:admin> cfgremove "Test_cfg", "redzone"
```

See Also

```
cfgadd
cfgclear
cfgcreate
cfgdelete
cfgdisable
cfgenable
cfgsave
cfgshow
cfgtransabort
cfgtransshow
```

cfgsave

Save zone configuration to non-volatile (flash) memory.

Syntax `cfgsave`

Availability Admin

This command requires a zoning license.

Description Use this command to save the current zone configuration. The defined configuration and the name of the enabled configuration are written to flash memory in all switches in the fabric.

The saved configuration is automatically reloaded by the switch on power-up and, if a configuration was enabled at the time it was saved, the same configuration is reinstalled with an automatic `cfgenable` command.

Because the saved configuration is reloaded at power-up, only valid configurations are saved. `cfgsave` verifies that the enabled configuration is valid by performing the same tests as `cfgenable`. If the tests fail, an error is displayed and the configuration is not saved. Tests may fail if a configuration has been modified since the last `cfgenable`.

This command ends and commits the current transaction. If a transaction is open on a different switch in the fabric when this command is run, the transaction on the other switch is automatically aborted. A message is displayed on the other switch notifying the transaction abort.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To save a zone configuration:**

```
switch:admin> cfgsave
Updating flash...
```

See Also

`cfgadd`
`cfgclear`
`cfgcreate`
`cfgdelete`
`cfgdisable`
`cfgenable`
`cfgremove`
`cfgshow`
`cfgtransabort`
`cfgtransshow`

cfgshow

Display zone configuration information.

Syntax `cfgshow ["pattern"[, mode]`

Availability All users

This command requires a zoning license.

Description Use this command to display zone configuration information.

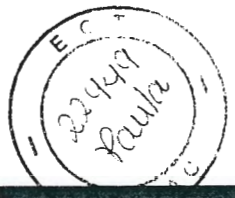
If no operand is specified, all zone configuration information (both Defined and Effective) is displayed.

If an operand is specified, it is used as a pattern to match zone configuration names in the defined configuration; those that match the pattern are displayed.

The defined configuration is the complete set of all zone objects that have been defined in the fabric. There can be multiple zone configurations defined, but only one can be enabled at a time. There may be inconsistencies in the definitions, zones or aliases that are referenced but not defined, or there may be duplicate members. The Defined configuration is the current state of the administrator input.

The Effective configuration is the single zone configuration that is currently enabled. The devices that an initiator sees in the fabric are based on this configuration. The Effective configuration is built when a specific zone configuration is enabled and all error checking has been completed successfully.

When security is enabled, this command can only be issued from the primary FCS switch.



Operands This command has the following operands:

"pattern" A POSIX-style regular expression used to match zone configuration names. The pattern must be enclosed in quotation marks. Patterns can contain:

- Question mark (?) that matches any single character.
- Asterisk (*) that matches any string of characters.
- Ranges that match any character within the range. For example, [0-9] or [a-f].

This operand is optional.

mode Specify `0` to display the contents of the transaction buffer (the contents of the current transaction), or specify `1` to display the contents of the non-volatile memory. The default value is `0`. This operand is optional.

Example **To show all zone configurations that start with "Test":**

```
switch:admin> cfgshow "Test*"
cfg:    Test1 Blue_zone
cfg:    Test_cfg Red_zone; Blue_zone
```

To show all zone configuration information:

```
switch:admin> cfgshow
   Defined configuration:
     cfg:    USA1     Blue_zone
     cfg:    USA_cfg Red_zone; Blue_zone
     zone:   Blue_zone
        1,1; array1; 1,2; array2
     zone:   Red_zone
        1,0; loop1
     alias: array1   21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
     alias: array2   21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
     alias: loop1    21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

   Effective configuration:
     cfg:    USA_cfg
     zone:   Blue_zone
         1,1
         21:00:00:20:37:0c:76:8c
         21:00:00:20:37:0c:71:02
         1,2
         21:00:00:20:37:0c:76:22
         21:00:00:20:37:0c:76:28
      zone:   Red_zone
         1,0
         21:00:00:20:37:0c:76:85
         21:00:00:20:37:0c:71:df
```

To show only configuration names:

```
switch:admin> cfgshow *
 cfg:    a_cfg1 zone1; zone2
 cfg:    b_cfg2 zone1; zone2; zone3

switch:admin>
```

See Also

cfgadd
cfgclear
cfgcreate
cfgdelete
cfgdisable
cfgenable
cfgremove
cfgsave
cfgtransabort
cfgtransshow

cfgsize

Display the size details of the zone database.

Syntax `cfgsize [integer]`

Availability All users

This command requires a zoning license.

Description Use this command to display the size details of the zone database.

The size details include the Zone DB max size, the committed size, and the transaction size. All sizes are in bytes.

The 'Zone DB max size' is the upper limit for the Defined configuration, determined by the amount of flash memory available for storing the Defined configuration.

The 'committed size' is the size of the Defined configuration currently stored in flash.

The 'transaction size' is the size of the uncommitted Defined configuration. This value will be non-zero if the Defined configuration is being modified by telnet, API etc; otherwise it is 0.

Refer to `cfgshow` for a description of Defined and Effective configurations.

When security is enabled, this command can be issued from any switch in the fabric.

Operands This command has the following operand:

integer	If a non-zero integer is specified as the parameter, the size of the flash memory allocated for the zone database is displayed. The zone database includes both the Defined and Effective configurations. This size is in kilobytes. This operand is optional.

Example **To display size details of the Defined configuration:**

```
switch:admin> cfgsize
Zone DB max size - 127726 bytes
```

```
committed - 8812
transaction - 0
switch:admin> cfgsize 1
Zone DB flash size - 131028 bytes
switch:admin>
```

See Also `cfgshow`

cfgtransabort

Abort the current zoning transaction.

Syntax `cfgtransabort [token]`

Availability Admin

This command requires a zoning license.

Description Use this command to abort the current zoning transaction without committing it. All changes made since the transaction was started are removed and the zone configuration database restored to the state before the transaction was started.

If a transaction is open on a different switch in the fabric when this command is run, the transaction on the other switch remains open and unaffected.

When security is enabled, this command can only be issued from the primary FCS switch.

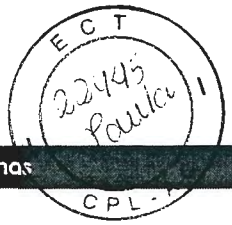
Operands This command has the following operand:

token	Specify the token ID of an abortable transaction. Use the cfgtransshow command to obtain the token ID of a transaction

Example To abort the current transaction:

```
switch:admin> cfgtransabort
```

See Also
`cfgadd`
`cfgclear`
`cfgcreate`
`cfgdelete`
`cfgdisable`



```
cfgenable
cfgremove
cfgsave
cfgshow
cfgtransabort
cfgtransshow
```

cfgtransshow

Display information about the current zoning transaction.

Syntax `cfgtransshow`

Availability Admin

This command requires a zoning license.

Description Use this command to show the ID of the current transaction. It will indicate whether the transaction is abortable. The transaction cannot be aborted if it is an internal zoning transaction.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To display information about the current transaction:**

```
switch:admin> cfgtransshow
There is no outstanding zone transactions
switch:admin> cfgclear
Do you really want to clear all configurations?  (yes, y,
   no, n): [no] y
Clearing All zoning configurations...
switch:admin> cfgtransshow
Current transaction token is 271010736
It is abortable
switch:admin>
```

See Also

```
cfgadd
cfgclear
cfgcreate
cfgdelete
cfgdisable
cfgenable
cfgremove
cfgsave
```

```
cfgshow
cfgtransabort
```

chassisname

Display or set the chassis name for an ED-12000B.

Syntax `chassisname [name]`

Availability Admin (set)

All users (display)

Description Use this command to change the name associated with the chassis ED-12000B. In the ED-12000B, there are two logical switches associated with a single chassis.

Enter this command with no parameter to display the current name.

Enter this command with a name specified to set the chassis name to the new value.

Operands This command has the following operand:

name	Specify a new name for the chassis. Chassis names can be up to 15 characters long and must begin with a letter. The name must consist of letters, digits or underscore characters.

Example **To change the chassis's name to "echo":**

```
switch:admin> chassisname echo
Please wait while committing configuration...
switch:admin>
```

See Also `switchname`

chassisshow

Display all field replaceable units (FRUs).

Syntax `chassisshow`

Availability All users

Description Use this command to inventory and display the field replaceable unit (FRU) header content for each object in the chassis. On some platforms for certain FRU types, a few items may not be available. In these cases the lines will be suppressed. Possibly affected are lines 2, 3, 4, 5, 6, 8, and 10 through 13. In addition, for lines 10 through 13, if there is no data set, these lines will be suppressed.

The header data is formatted into a record consisting of (up to) 13 lines. The lines and their meaning are shown in Table 1-1. (Refer also to the `chassisShow` example.).

Table 1-1 ChassisShow Line Numbers

Line Number	Description	Example
1	Contains object ID.	Object type: CHASSIS, FAN, POWER SUPPLY, SW BLADE (switch) CP BLADE (Control Processor), WWN (World Wide Name), or UNKNOWN; and Object number: Slot <nn> (for blades) Unit <nn> (for everything else) If the FRU is part of an assembly, a brief description in parenthises will be displayed
2	Displays FRU header version number.	Header Version: <*x*>
3	Displays the value used to calculate the object's power consumption; positive for power supplies; negative for consumers.	Power Consume Factor: <*-xxx*>
4	Displays ED-12000B part number (up to 14 characters).	ED-12000B Part Num: <*xx-yyyyyyy-zz*>
5	Displays ED-12000B serial number (up to 12 characters).	Ed-12000B Serial Num: <*xxxxxxxxxx*>

Table 1-1 ChassisShow Line Numbers (*continued*)

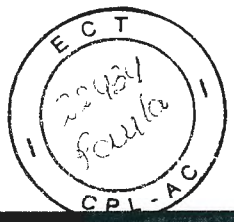
6	Displays the date the FRU was manufactured.	Manufacture: Day: <*dd*> Month: <*mm*> Year: <*yyyy*>
7	Displays the date the FRU header was last updated.	Update: Day: <*dd*> Month: <*mm*> Year: <*yyyy*>
8	Displays cumulative time, in days, that the FRU has been powered on.	Time Alive: <*dddd*> days
9	Displays the current time, in days, since the FRU was last powered on.	Time Awake: <*dddd*> days
10	Displays the externally supplied ID (up to 10 characters)	ID: <*xxxxxxxxxx*>
11	Displays the externally supplied part number (up to 20 characters).	Part Num: <*xxxxxxxxxxxxxxxxxxxx*>
12	Displays the externaly supplied serial number (up to 20 characters).	Serial Num: <*xxxxxxxxxxxxxxxxxxxx*>
13	Displays the externally supplied revision number (up to 4 characters).	Revision Num: <*xxxx*>

Operands None

Example To display all Field Replaceable Units for a switch:

```
switch12k:admin> chassisShow
   SW BLADE  Slot: 3
   Header Version:          1
   Power Consume Factor:    -180
   Brocade Part Num:        60-0001532-03
   Brocade Serial Num:      1013456800
   Manufacture:             Day: 12  Month:  6  Year: 2001
   Update:                  Day: 15  Month:  7  Year: 2001
   Time Alive:              28 days
   Time Awake:              16 days
   ID:                      555-374757
   Part Num:                234-294-12345
   Serial Num:              2734658
   Revision Num:            A.00

   CP BLADE  Slot: 6
   Header Version:          1
   Power Consume Factor:    -40
   Brocade Part Num:        60-0001604-02
   Brocade Serial Num:      FP00X600128
   Manufacture:             Day: 12  Month:  6  Year: 2001
   Update:                  Day: 15  Month:  7  Year: 2001
   Time Alive:              61 days
   Time Awake:              16 days
   ID:                      555-374757
   Part Num:                236-296-12350
   Serial Num:              2836542
   Revision Num:            A.00

   <output truncated>
```

See Also slotshow



chippropshow

Display ASIC chip property contents.

Syntax `chippropshow [slot/]chip | [[slot] number] -all`

Availability All users

Description Use this command to display the ASIC chip property contents for the specified chip on the specified blade.

The output of this command is only for support use only.

Operands This command has the following operands:

[slot/]chip	Specify the index of the chip within the blade to be displayed. The default is set to 0 and designed to operate on fixed port count products.
[[slot] *number*] -all	If specified, the chip property contents for the entire blade are displayed. The default is set to 0 and designed to operate on fixed port count products.

Example **To view the chip properties on blade:**

```
switch:admin> chippropshow --slot 1 -all
slot: 1, minis: 0, chip: 0
[1657/0001,0104,2/8]
slot: 1, minis: 0, chip: 1
[1657/0001,0104,2/8]
slot: 1, minis: 1, chip: 0
[1657/0001,0104,2/8]
slot: 1, minis: 1, chip: 1
[1657/0001,0104,2/8]
slot: 1, minis: 2, chip: 0
[1657/0001,0104,2/8]
slot: 1, minis: 2, chip: 1
[1657/0001,0104,2/8]
slot: 1, minis: 3, chip: 0
[1657/0001,0104,2/8]
slot: 1, minis: 3, chip: 1
[1657/0001,0104,2/8]
```

See Also `ptpropshow`

chipregshow

Display port registers of a given chip number.

Syntax `chipregshow [slot/]chip [filter]`

Availability All users

Description Use this command to display the ASIC register contents for the specified chip on the specified blade slot.

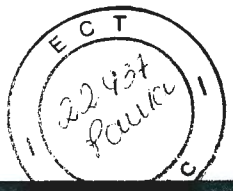
The output of this command is only for support use only.

Operands This command has the following operands:

[slot/]chip	Specify the index of the chip within the specified blade to be displayed. The default is set to 0 and designed to operate on fixed port count products.
filter	Specify a filter string.

Example **To display the port registers of chip:**

```
switch:admin> chipregshow 1/1 ffffffff
Port Registers for slot: 1, port: 8
0xc9b8803c: toc_ctl         0000         0xc9b88044: ...
0xc9b8804c: flist_stat      0018037e     0xc9b88054: ...
0xc9b8805c: plist_stat      ffffffff     0xc9b88064: ...
0xc9b8806c: aulist_stat     ffffffff     0xc9b88070: ...
0xc9b8aca4: port_speed      ffffffff     0xc9b8aca8: ...
0xc9b8acb6: epi2_stat       0000         0xc9b8acc4: ...
0xc9b8accc: listB_stat      ffffffff     0xc9b8acdc: ...
0xc9b8d4c8: frzfrm_did      00ad0701     0xc9b8d4cc: ...

Port Registers for slot: 1, port: 9
0xc9b9803c: toc_ctl         0000         0xc9b98044: ...
0xc9b9804c: flist_stat      0018037e     0xc9b98054: ...
0xc9b9805c: plist_stat      ffffffff     0xc9b98064: ...
0xc9b9806c: aulist_stat     ffffffff     0xc9b98070: ...
0xc9b9aca4: port_speed      ffffffff     0xc9b9aca8: ...
0xc9b9acb6: epi2_stat       0000         0xc9b9acc4: ...
0xc9b9accc: listB_stat      ffffffff     0xc9b9acdc: ...
0xc9b9d4c8: frzfrm_did      00ad0301     0xc9b9d4cc: ...
--- <output truncated> ---
```



See Also `chippropshow`
`ptregshow`

cmemretentiontest

Run data retention test of the central memory SRAMs.

Syntax `cmemretentiontest [-slot` *`number`*`] [-passcnt` *`count`*`] [-datatype` *`type`*`] [-ports` *`itemlist`*`] [-seed` *`value`*`]`

Availability Admin

Description Use this command to verify that data written into the central memory SRAMs in the ASIC pair is retained after a 10 second wait. The method used is to write a fill-pattern to all SRAMs, wait 10 seconds, and then read all SRAMs, to verify that the data read matches the data previously written. The process is then repeated using the reverse version of the pattern.

This command may not be executed on an enabled switch. You must first disable the switch using the `switchdisable` command.

Operand This command has the following operand:

`-slot` *number* Specify the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is set to `0` and designed to operate on fixed port count products.

`-passcnt` *count* Specify the number of test passes to run. By default the test will be run one time.

`-datatype type`

Specify the type of data pattern to use. By default, type 9, QUAD_RAMP is used. For a complete list of supported data patterns run the `datatypeshow` command. Some common settings are:

Pattern	Type	Example
BYTE_FILL	1	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
WORD_FILL	2	0000 0000 0000 0000 0000 0000 0000 0000
QUAD_FILL	3	00000000 00000000 00000000 00000000
QUAD_RAMP	9	00000000 00000001 00000002 00000003
RANDOM	11	55 16 fc d7 17 65 a9 87 5f 44 be 5a d0 de bc a5

`-ports` *itemlist* Specify a set of ports to test. Specify a list of blade ports to test. The Ports list is translated into a matching quad list before the test is run. By default all the blade ports in the specified slot (`-slot`) are tested. See the `itemlist` help pages for further details.

`-seed` *value* Specify the data pattern seed to be used. The default seed value is `0`.

Example **To run the data retention test on the central memory SRAMS:**

```
switch:admin> cmemretentiontest --slot 3
Running cmemretentiontest ..............
Test Complete: cmemretentiontest Pass 2 of 2
Duration 0 hr, 2 min & 13 sec (0.2:13:234
 passed.
```

Errors Below are possible error messages if failures are detected

```
LCMEM_ERR
LCMRS_ERR
LCMTO_ERR
```

See Also

```
camtest
centralmemorytest
cmitest
crossporttest
datatypeshow
itemlist
portloopbacktest
spinsilk
sramretentiontest
```

cmitest

Verify the Control Message Interface (CMI) bus between ASICs

Syntax

```
cmitest [-slot number][-passcnt count][-txports
list][-rxports list][-skip mask]
```

Availability

Admin

Description

Use this command to test:

- the multiplexed 4-bit CMI point-to-point connection between two ASICs.
- the message sent with a bad checksum will set the error and interrupt bits of the destination ASIC.
- a message with a good checksum will not set any error or interrupt bit in any ASIC pair.

The Control Message Interface (CMI) is used to send transmission requests or completion messages between the ASIC transmitter and receiver.

Options

This command has the following options:

`-slot number` Specify the slot number to test. The default is set to 0 and designed to operate on fixed port count products.

`-passcnt count` Specify the number of test passes to run. By default the test will be run one time.

`-txports list` Specify a list of ports to transmit data. By default all the ports in the specified slot (`--slot number`) will be used. See `itemlist` help pages for further details.

`-rxports list` Specify a list of ports to receive data. By default all the ports in the specified slot (`-slot number`) will be used. See `itemlist` for more information.

`-skip mask` Specify the particular test by using the following bit weight data:

- 1 CMI data test (ignore checksum
- 2 CMI checksum test
- 3 Enable all tests

This operand is optional.

Example **Run a CMI test between two ASIC pairs:**

```
switch:admin> cmitest -txports 3/0-3/7 -rxports 3/8-3/15
Running cmitest ..............
Test Complete: cmitest Pass 1 of 1
Duration 0 hr, 0 min & 2 sec (0:0:2:591).
passed.
```

Errors Listed below are possible error messages if failures are detected:

```
DIAG-BADINT
DIAG-CMICKSUM
DIAG-CMIDATA
DIAG-CMIINVCAP
DIAG-CMINOCAP
DIAG-CMISA1
DIAG-INTNIL
```

See Also

```
camtest
centralmemorytest
cmemretentiontest
crossporttest
itemlist
portloopbacktest
portregtest
spinsilk
sramretentiontest
```

configdefault

Reset the configuration settings to the default values.

Sytax `configdefault`

Availability Admin

Description Use this command to reset a subset of configuration settings to the default values.

All configuration parameters, with the following exceptions, are reset to default values:

- Ethernet MAC address, IP address, and subnetmask
- IP gateway address
- License keys
- OEM customization
- SNMP configuration
- System name
- World Wide Name
- Brocade Advanced Zoning configuration

Some configuration parameters are cached by the system. To avoid unexpected switch behavior, reboot the system after executing this command.

Refer to the `configure` command for more information on default values for configuration parameters.

This command may not be executed on an enabled switch. You must first disable the switch using the `switchdisable` command.

Operands None.

Example **To restore the system configuration to default values:**

```
switch:admin> configdefault
Committing Configuration ...done.
```

See Also

```
agtcfgdefault
configure
```

```
switchdisable
switchenable
```

configdownload

Download a switch configuration file from a host system.

Sytax `configdownload ["host","user","file","passwd"]`

Availability admin

Description Use this command to download a switch configuration file from a host system. The configuration file is ASCII text and may have been generated using `configupload`, or it may have been created by a user to download specific configuration changes. The download process uses FTP.

Fabric OS v4.x only supports FTP. In Fabric OS v4.x no spaces are allowed between operands.

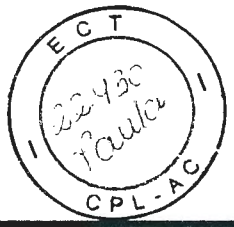
To restore the configuration file from a Windows NT system using FTP, the FTP server may have to be installed from the distribution media and enabled.

This command can be invoked without any operands, and becomes an interactive session.

The download process is additive; that is, the lines read from the file are added to the current switch configuration. This enables you to change a single configuration variable by downloading a file with a single line. All other variables remain unchanged. This is particularly important when downloading a zoning configuration. Since the new zoning information is added to the current configuration, there may not be any conflicts. Typically this command is used to add a consistent change to the current zoning configuration, or to replace the current zoning configuration, in which case `cfgclear` must be invoked before `configdownload`.

When the switch is in secure mode, the following rules and restrictions apply:

- Both Defined Security policies and Active Security policies sections must exist and contain the FCS_POLICY;



- In the Defined Security policies section, at least one member of the FCS_POLICY must be the same as a member in the previous FCS_POLICY;
- In the Active Security policies section, the FCS_POLICY must be exactly the same as the previous FCS_POLICY.
- Order of members must be maintained;
- If either security policies section has a RSNMP_POLICY, then that section must have a WSNMP_POLICY;
- After the switch is enabled, if the switch is the Primary FCS, then its security and zoning information will be propagated to all other switches in the fabric;
- After the switch is enabled, if the switch is a non-FCS or a backup FCS, then its security and zoning information will be overwritten by the Primary FCS.

A license key is only accepted if the boot.mac line matches the WorldWide Name of the switch performing the download, otherwise it is ignored.

A switch's identity cannot be changed by `configdownload`. These parameters (such as the switch's name and IP address) are ignored.

If the configuration file contains the keyword `enable: <zone_configuration>`, then that zoning configuration will be enabled in the fabric. If there is no `enable` keyword in the configuration file or no zoning configuration by that name exists or if enable fails for any reason (such as dangling aliases), then:

- The Effective Configuration will remain as what it was prior to the `configdownload`. That is, all the "enable" information is discarded.
- The Defined Configuration will change to reflect new zoning configuration.

Operands This command has the following operands:

host Specify a host name or IP address in quotation marks; for example, `citadel` or `192.168.1.48`. The configuration file is downloaded from this host system. This operand is optional.

user	Specify a user name in quotation marks; for example, `jdoe`. This user name is used to gain access to the host system. This operand is optional.
file	Specify a file name in quotation marks; for example, `config.txt`. Absolute path names may be specified using forward slash (/). Relative path names search for the file in the user's home directory on UNIX hosts, and in the directory where the FTP server is running on Windows hosts. This operand is optional.
passwd	Specify a password in quotation marks. This operand is optional.

Example **To load a backup configuration file from a host system:**

```
switch:admin> configdownload
   "123.123.123.123","jdoe","config.txt", "password1"
Committing configuration...done.
download complete
```

If you enter the command with no operands, you are prompted for the appropriate values:

```
switch:admin> configdownload
Server Name or IP Address [host]: 123.123.123.123
User Name [None]: user21
File Name [config.txt]: config-switch.txt
Password: xxxxxxxxx
download complete
switch:admin>
```

Errors Listed below are possible reasons for a failure of this command:

- The host name is not known to the switch
- The host IP address cannot be contacted
- The user does not have permission on the host
- The user runs a script that prints something at login
- The file does not exist on the host
- The file is not a switch configuration file
- The FTP server is not running on the host
- The configuration data contains errors.

See Also

```
configdefault
configupload
configshow
```

configure

configshow

Display system configuration settings.

Syntax `configshow ["filter"]`

Availability All users.

Description Use this command to view the system configuration settings set by the `configure` command.

Operands This command has the following operand:

filter Specify a text string in quotation marks that limits the output of the command to only those entries that contain the text string. This operand is optional.

Example **To display system configuration settings:**

```
switch:admin> configshow
diag.postDisable:        0
fabric.domain:  1
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.tachyonCompat:   0
fabric.ops.mode.unicastOnly:     0
fabric.ops.mode.useCsCtl:        0
fabric.ops.mode.vcEncode:        0
fabric.ops.vc.class.2:   2
fabric.ops.vc.class.3:   3
fabric.ops.vc.config:    0xc0
fabric.ops.vc.linkCtrl:  0
fabric.ops.vc.multicast:         7
fc4.fcIp.address:        192.168.65.62
fc4.fcIp.mask:   255.255.255.0
fcAL.fanFrameDisable:    0
fcAL.useAltBBCredit:     0
lcdContrast:     128
licenseKey:      none
rpc.rstatd:      1
rpc.rusersd:     1
```

Configuration parameters vary depending on system model and configuration.

See Also

`agtcfgshow`
`configure`
`diagdisablepost`
`diagenablepost`
`ipaddrshow`
`licenseshow`
`syslogdipshow`

configupload

Create a backup file of switch configuration information on a host workstation.

Syntax `configupload ["host","user","file"[,"passwd"]]`

Availability Admin

Description Use this command to upload the switch configuration to a host file. The upload process uses FTP.

If the command is entered without operands, it becomes interactive and prompts the user for input.

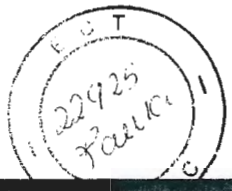
The configuration file is written as three sections. The first section contains the switch boot parameters. It has variables such as the switch's name and IP address. This section corresponds to the first few lines of output of the `configshow` command.

The second section contains general switch configuration variables, such as diagnostic settings, fabric configuration settings, and SNMP settings. This section corresponds to the output of the `configshow` command (after the first few lines), although there are more lines uploaded than shown by the command.

The third sections contains the zoning configuration parameters.

In Fabric OS v4.x no spaces are allowed between operands. None of the operands, the host, user, file name, or password can use the double quote character (").

Operands This command has the following operands:



host	Specify a host name or IP address in quotation marks; for example, `citadel` or `192.168.1.48`. The configuration file is downloaded from this host system. This operand is optional.
user	Specify a user name in quotation marks; for example, `jdoe`. This user name is used to gain access to the host. This operand is optional.
file	Specify a file name in quotation marks; for example, `config.txt`. Absolute path names may be specified using forward slash (/). Relative path names create the file in the user's home directory on UNIX hosts, and in the directory where the FTP server is running on Windows hosts. This operand is optional.
passwd	Specify a password in quotation marks. This operand is optional.

Example

To create a backup file of switch configuration information:

```
switch:admin> configupload
   "123.123.123.123","jdoe","config.txt","password1"
upload complete
switch:admin>
```

If you enter the command with no operands, you are prompted for the appropriate values:

```
switch:admin> configupload
Server Name or IP Address [host]: 123.123.123.123
User Name [None]: user21
File Name [config.txt]: config-switch.txt
Password: xxxxxxxx
upload complete
switch:admin>
```

Errors

Listed below are possible reasons for a failure of this command:

- The host name is not known to the switch
- The host IP address cannot be contacted
- The user does not have permission on the host
- The user runs a script that prints something at login
- The FTP server is not running on the host

See Also

`configdefault`
`configdownload`
`configshow`

configure

Modify system configuration parameters.

Syntax `configure`

Availability Admin

Description Use this command to change the following system configuration parameters:

- Fabric Parameters
- Virtual Channel Settings
- Zoning Operation Parameters
- Rscn Transmission Mode
- NS Pre-zoning Mode
- Arbitrated Loop Parameters
- System Services
- Portlog Events Enable

This command can now be executed on an enabled switch. If executed on an enabled switch only a subset of the full parameter set is available. To access all parameters controlled by this command, you must disable the switch.

The `configure` command is navigated using a series of menus. Top level menus, and associated submenus consist of a text prompt, a list of acceptable values, and a default value (in brackets).

Use the following options to control input:

Return — When entered at a prompt with no preceding input, accepts the default value (if applicable) and moves to the next prompt.

Interrupt (control-C) — Aborts the command immediately and ignores all changes made.This keystroke is common on many computers, but can be different on your system.

End-of-file (control-D)
When entered at a prompt with no preceding input, terminates the command and saves changes made.This keystroke is common on many computers, but may be different on your system.

Fabric Parameters

There are a number of settings which control the overall behavior and operation of the Fabric. Some of these values, such as the domain, are assigned automatically by the fabric and may differ from one switch to another in the fabric. Other parameters, such as the BB credit, can be changed for specific applications or operating environments, but *must* be in agreement among all switches to allow formation of the fabric.

The fabric parameters are shown in Table 1-2.

Table 1-2 Configure Command Fabric Parameters

Field	Default	Range
Domain	1	1..239
R_A_TOV	10000	4000..120000
E_D_TOV	2000	1000 to 5000
Data Field Size	2112	256 to 2112
Sequence Level Switching	0	0 or 1
Disable Device Probing	0	0 or 1
Suppress Class F Traffic	0	0 or 1
VC Encoded Address Mode	0	0 or 1
Per-frame Route Priority	0	0 or 1
Long Distance Fabric	0	0 or 1
BB Credit	16	1 to 16

Descriptions of the switch fabric setting fields are as follows:

Domain — The domain number uniquely identifies the switch in a Fabric. This value is automatically assigned by the Fabric. The range of valid values varies depending on the switch model and other system parameter settings.

R_A_TOV — The Resource Allocation Time Out Value (R_A_TOV) is displayed in milliseconds. This variable works with the variable E_D_TOV to determine switch actions when presented with an error condition.

Allocated circuit resources with detected errors are not released until the time value has expired. If the condition is resolved prior to the time out, the internal time out clock resets and waits for the next error condition.

E_D_TOV — Error Detect Time Out Value (E_D_TOV) is displayed in milliseconds. This timer is used to flag a potential error condition when an expected response is not received (an acknowledgment or reply in response to packet receipt, for example) within the set time limit. If the time for an expected response exceeds the set value, then an error condition occurs.

Data Field Size — The data field size specifies the largest possible value, in bytes, and advertises this value to other switches in the fabric during construction of the fabric as well as to other devices when they connect to the fabric. Setting this to a value smaller than 2112 may result in decreased performance.

Sequence Level Switching

When Sequence Level Switching is set to 1, frames of the same sequence from a particular source are transmitted together as a group. When this feature is set to 0, frames are transmitted interleaved among multiple sequences.

Under normal conditions, Sequence Level Switching should be disabled for better performance. However, some host adapters have performance issues when receiving interleaved frames from multiple sequences. When there are such devices attached to the fabric, Sequence Level Switching should be enabled.

Disable Device Probing

When Disable Device Probing is set to 1, devices that do not register with the Name Server are not present in the Name Server data base. Set this mode only if the switch N_Port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail.

Suppress Class F Traffic

When this mode is set to 1, all class F interswitch frames are transmitted as class 2 frames. This is to support remote fabrics which involve ATM gateways which don't support class F traffic.

VC Encoded Address Mode

When VC Encoded Address Mode is set to 1, frame source and destination address utilize an address format compatible with SilkWorm 1000 series switches. Set this mode only if the fabric includes this type of switch. This mode cannot be set if security mode is enabled. Likewise, security mode cannot be enabled if VC Encoding Address Mode is enabled. Use the secmodeshow command to view the security mode.

Per-frame Route Priority

In addition to the eight virtual channels used in frame routing priority, support is also available for per-frame based prioritization when this value is set. When Per-frame Route Priority is set to 1, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.

Long Distance Fabric

When this mode is set to 1, ISLs in a fabric can be up to 100Km long. The exact distance level is determined by the per-port configuration on the E_Ports of each ISL. Both E_Ports in an ISL must be configured to run the same long distance level, otherwise, the fabric will be segmented. The Extended Fabric License is required to set this mode.

BB Credit

The buffer-to-buffer (BB) credit represents the number of buffers available to attached devices for frame receipt. The range of allowed values varies depending on other system settings

Virtual Channel Settings

The switch enables fine tuning for a specific application, by configuring the parameters for eight virtual channels. The first two virtual channels are reserved for switch internal functions and are not available for modification.

The default virtual channel settings have already been optimized for switch performance. Changing the default values can improve switch performance, but can also degrade performance. Do not change these settings without fully understanding the effects of the changes.

The Virtual Channel Setting fields are shown in Table 1-3.

Table 1-3 Configure Command Virtual Channel Settings

Field	Default	Range
VC Priority 2	2	2 to 3
VC Priority 3	2	2 to 3
VC Priority 4	2	2 to 3
VC Priority 5	2	2 to 3
VC Priority 6	3	2 to 3
VC Priority 7	3	2 to 3

Descriptions of the Virtual Channel Setting fields are as follows:

VC Priority — Specifies the class of frame traffic given priority for a Virtual Channel.

Zoning Operation Parameters

The Zoning Operation Parameter fields are as follows:

Disable NodeName Zone Checking

Specify 1 to disable using Node WWN when specifying nodes in the zone database, or specify 0 to enable using Node WWN when specifying nodes in the zone data. The default value is 0. This value must be set to 1 for interoperability.

RSCN Transmission Mode

The RSCN Transmission Mode fields are as follows:

End-device RSCN Transmission Mode
: Specify 0 for RSCN with single PID, 1 for RSCN with multiple PIDs, or 2 Fabric RSCN. The default value is 0.

NS Operation Parameters

The NS Pre-zoning Mode fields are as follows:

Pre-zoned responses Mode
: Specify 0 for Standard Mode, or 1 for Pre-zoning On. The default value is 0.

Arbitrated Loop Parameters

The Arbitrated Loop Setting fields are shown in Table 1-4.

Table 1-4 Configure Command Arbitrated Loop Settings

Field	Default	Range
Alternate BB Credit?	0	0 or 1
Send FAN frames?	1	0 or 1
Enable CLOSE on OPEN received?	0	0 or 1
Always send RSCN?	0	0 or 1
Do Not Allow AL_PA 0x00?	0	0 or 1

Descriptions of the Arbitrated Loop Parameter fields are as follows:

Send FAN frames?
: Specifies that fabric address notification (FAN) frames be sent to public loop devices to notify them of their node ID and address. When set to 1, frames are sent; when set to 0 frames are not sent.

Enable CLOSE on OPEN received?
: If this is set, a CLS is returned immediately to an OPN if no buffers are available. This is required for TachLite.

Always send RSCN?
: Following the completion of loop initialization, a remote state change notification (RSCN) is issued when FL_Ports detect the presence of new devices or

the absence of pre-existing devices. When set, a RSCN is issued upon completion of loop initialization, regardless of the presence or absence of new or pre-existing devices.

Do Not Allow AL_PA 0x00?
This option disables ALPA values from being 0x00.

System Services

The System Services fields are shown in Table 1-5.

Table 1-5 Configure Command System Services Parameters

Field	Default	Range
rstatd	Off	On/Off
rusersd	Off	On/Off
telnetd	On	On/Off
rapid	On	On/Off
thad	On	On/Off
Disable RLS probing	On	On/Off

Descriptions of the system service setting fields are as follows:

`rstatd` Dynamically enables or disables a server that returns information about system operation information through remote procedure calls (RPC). The protocol provides for a wide-range of system statistics.

The retrieval of this information is supported by a number of operating systems which support RPC. Most UNIX-based systems (HP-UX, Irix, Linux, Solaris, etc.) use the rup and rsysinfo commands to retrieve the information. See your local system documentation for the appropriate usage of the these or equivalent commands.

`rusersd` Dynamically enables or disables a server that returns information about the user logged into the system through remote procedure calls (RPC). The information returned includes user login name, the system name, login protocol or type, login time, idle time, and remote login location (if applicable).

The retrieval of this information is supported by a number of operating systems which support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, etc.) the command to retrieve the information is rusers. See your local system documentation for the appropriate usage of this or equivalent command.

`telnetd` Used to enable or disable the telnet interface to a switch, including sectelnet. If you are using SSH to manage a switch you can disable the telnet interface for greater security. The default value is on (telnet is enabled).

`rapid` Dynamically enables or disables a service that handles RPC requests for the API server. The default value is on.

`thad` Dynamically enables or disables the threshold monitor. The default value is on.

`Disable RLS probing`
This disables Read Link Error Status probing of the ALPAs. The default value is on, that is, Disable RLS probing is disabled.

Portlog Events Enable

Use these parameters to specify which events create an entry in the port log. The Portlog Events fields are shown in Table 1-6.

Table 1-6 Configure Command Portlog Events Parameters

Field	(Valid Values) Default Value
`start: a switch start or re-start event`	(on, off): [on]
`disable: a port is disabled`	(on, off): [on]
`enable: a port is enabled`	(on, off): [on]
`ioctl: a port I/O control is executed`	(on, off): [on]
`Tx: a frame is transmitted`	(on, off): [on]
`Tx1: a frame is transmitted, class 1`	(on, off): [on]
`Tx2: a frame is transmitted, class 2`	(on, off): [on]

Table 1-6 Configure Command Portlog Events Parameters (*continued*)

Field	(Valid Values) Default Value
Tx3: a frame is transmitted, class 3	(on, off): [on]
Rx: a frame is received	(on, off): [on]
Rx1: a frame is received, class 1	(on, off): [on]
Rx2: a frame is received, class 2	(on, off): [on]
Rx3: a frame is received, class 3	(on, off): [on]
stats: port status or statistics	(on, off): [on]
scn: a state change notification	(on, off): [on]
pstate: a port changes physical state	(on, off): [on]
reject: a received frame is rejected	(on, off): [on]
busy: a received frame is busied	(on, off): [on]
ctin: a CT based request is received	(on, off): [on]
ctout: a CT based response is transmitted	(on, off): [on]
errlog: a message is added to the error log	(on, off): [on]
loopscn: a loop state change notification	(on, off): [on]
create: a task is created	(on, off): [on]
debug: generic debug info	(on, off): [on]
nbrfsm: neighbor state transition	(on, off): [on]
timer: timer	(on, off): [on]
sn: speed negotiation state	(on, off): [on]
fcin: Fibre Channel input	(on, off): [on]
fcout: Fibre Channel ouput	(on, off): [on]
read: Fibre Channel read	(on, off): [on]
write: Fibre Channel write	(on, off): [on]
err: Fibre Channel error	(on, off): [on]

Table 1-6 Configure Command Portlog Events Parameters *(continued)*

Field	(Valid Values) Default Value
frame: Fibre Channel frame payload	(on, off): [on]
msRemQ: inter-sw MS query	(on, off): [on]
msRemR: inter-sw MS response	(on, off): [on]
nsRemQ: inter-sw NS query	(on, off): [on]
nsRemR: inter-sw NS response	(on, off): [on]
rscn: RSCN	(on, off): [on]
state: Fibre Channel state	(on, off): [on]
xalloc: alloc an exchange	(on, off): [on]
xfree: free an exchange	(on, off): [on]
xerr: exchange error	(on, off): [on]
xstate: exchange state	(on, off): [on]
seq: sequence	(on, off): [on]
seqst: sequence state	(on, off): [on]
iu: iu	(on, off): [on]
payload: frame payload	(on, off): [on]
zone: zone request/response	(on, off): [on]
cmd: fss command log	(on, off): [on]
event: fss event log	(on, off): [on]
msg: fss message log	(on, off): [on]

Operands None

Example **To set the configuration parameters for a switch:**

```
switch:admin> configure

Configure...

Fabric parameters (yes, y, no, n): [no] yes
```

```
    Domain: (1..239) [3] 5
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112]
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0]
    VC Encoded Address Mode: (0..1) [0]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..16) [16]

Virtual Channel parameters (yes, y, no, n): [no] y

    VC Priority 2: (2..3) [2]
    VC Priority 3: (2..3) [2]
    VC Priority 4: (2..3) [2]
    VC Priority 5: (2..3) [2]
    VC Priority 6: (2..3) [3]
    VC Priority 7: (2..3) [3]

Switch Operating Mode (yes, y, no, n): [no]
Zoning Operation parameters (yes, y, no, n): [no]
RSCN Transmission Mode (yes, y, no, n): [no]
Arbitrated Loop parameters (yes, y, no, n): [no]
System services (yes, y, no, n): [no]
Portlog events enable (yes, y, no, n): [no]
Committing configuration...done.

switch:admin>
```

See Also

```
configdefault
configshow
ipaddrset
syslogdip
```

crossporttest

Functional test of port external transmit and receive path.

Syntax

`crossporttest [-nframes` *`count`*`] [-lb_mode` *`mode`*`] [-spd_mode` *`mode`*`] [-norestore` *`mode`*`] [-ports` *`itemlist`*`]`

Availability

Admin

Description

This command verifies the intended functional operation of the switch by sending frames from port M's transmitter, and looping the frames back through an external fiber cable into another port N's receiver; thus exercising all the switch components from the main

board, to the media, to the fiber cable, to the media, and back to the main board. With `-lb_mode` set to 1 it is also possible to test ports with loopback plugs that connect each port back to itself.

The cables can be connected to any port combination with the one condition; the cables and media connected must be of the same technology. This means a short wave length media port must be connected to another short wave length media port using a short wave length cable; and a long wave length port must be connected to a long wave length port; and a copper port must be connected to a copper port.

For best coverage, ports connected should be from different ASICs. For example, Ports 0-3 belong to ASIC 0, ports 4-7 belong to ASIC 1, etc. A connection from port 0 to port 15 exercises the transmit path between ASICs. A connection from port 0 to port 3 tests only the internal transmit path in ASIC 0.

Only one frame is transmitted and received at any one time. The port LEDs flicker green rapidly while the test is running.

The test method is as follows:

1. Determine which ports are connected to each other.
2. Enable ports for cabled loopback mode.
3. Create a frame F of maximum data size (2112 bytes).
4. Transmit frame F through port M.
5. Pick up the frame from its cross connected port N. An error is reported if any port other than N actually received the frame.
6. Check if any of the 8 statistic error counters are non-zero: ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.
7. Check if the transmit, receive or class 3 receiver counters are stuck at some value.
8. Check if the number of frames transmitted is not equal to the number of frames received.
9. Repeat steps 3 through 8 for all ports present until:
   - the number of frames requested is reached,
   - all ports are marked bad.

At each pass, a different data type is used to create the frame from a palette of 7; meaning if a pass of 7 is requested, 7 different frames are

used in the test. If 8 passes, the first 7 frames are unique, and the 8th is the same as the first. The data palette of 7 are:

```
CSPAT:        0x7e, 0x7e, 0x7e, 0x7e, ...
BYTE_LFSR:    0x69, 0x01, 0x02, 0x05, ...
CHALF_SQ:     0x4a, 0x4a, 0x4a, 0x4a, ...
QUAD_NOT:     0x00, 0xff, 0x00, 0xff, ...
CQTR_SQ:      0x78, 0x78, 0x78, 0x78, ...
CRPAT:        0xbc, 0xbc, 0x23, 0x47, ...
RANDOM:       0x25, 0x7f, 0x6e, 0x9a, ...
```

The `crossporttest` command behaves differently according to the modes activated.

SwitchEnable or SwitchDisable Mode

Online Mode

In ONLINE mode (where the switch is enabled prior to executing the `crossporttest` command) only ports which are cable loopbacked to ports in the same switch are tested. Ports connected outside of the switch are ignored.

To run the `crossporttest` command successfully the test must find at least one port (lb_mode = 1, this is the default) or two ports (lb_mode = 0) cable loopbacked to each other. If this criteria is not met, one of the following message is displayed:

```
Need at least 1 port(s) connected to run this test.
Need at least 2 port(s) cross-connected to run this
   test.
```

Offline Mode

In OFFLINE mode (when the switch is disabled prior to executing the `crossporttest` command) all ports are assumed to be cable loopbacked to different ports in the same switch. If one or more ports are not connected, the test aborts.

The test determines which port is connected to which port transmitting frames. If any ports are not properly connected (improperly seated SFPs or cables, bad SFPs or cables, or improper connection or improper connection of SWL to LWL), the following message is displayed:

```
One or more ports is not active, please double check
fibre channel connections on all ports.
```

Since this test includes the media and the fiber cable in its test path, its results combined with the results of `portloopbacktest` and `spinsilk` can be used to determine which components of the switch

are faulty. It is also possible to use loopback modes 3 and 5 to further isolate failures, see `-lb_mode` below.

Operands This command has the following operands:

`-nframes` *count* Specify the number of frames to send. The test will progress until the specified number of frames has been transmitted on each port. The default value is 10.

`-lb_mode` *mode* Specify the loopback mode for the test. By default, `crossporttest` uses mode 1 Port L loopback. Valid values are:

0 Cable Loopback
1 Port Loopback (loopback plugs)
2 External (SERDES) loopback
3 Silkscreen loopback
5 Internal (parallel) loopback

`-spd_mode` *mode* Specify the speed mode for the test. This parameter is only used for 2 Gbit/sec based products where it controls the speed at which each port is operated. For 1 Gbit/sec only products it is ignored. The exact operation of each mode 3 through 6 depends upon the loopback mode selected. When speed modes 3-6 are used with cables, they must be connected EVEN to ODD or the test will fail.

Valid values are:
0 Run test at both 1 Gbit/sec and 2 Gbit/sec
1 Lock all port speeds to 1 Gbit/sec
2 Lock all port speeds to 2 Gbit/sec

For `-lb_mode` set to 0 or 1, one of the following speed modes are available to test the speed negotiation:

3 Set all even ports speed to AN, set all odd ports speed to 1 Gbit/sec.

4 Set all even ports speed to AN, set all odd ports speed to 2 Gbit/sec.

5 Set all odd ports speed to AN, set all even ports speed to 1 Gbit/sec.

6 Set all odd ports speed to AN, set all even ports speed to 2 Gbit/sec.

For `-lb_mode` set to 2 or 3, the following speed modes are available to test FIFO underrun:

3,5 Set all even ports speed to 2 Gbit/sec, set all odd ports speed to 1 Gbit/sec.

4,6 Set all even ports speed to 1 Gbit/sec, set all odd ports speed to 2 Gbit/sec.

`-norestore` *mode* Specify 1 to force the test to skip part of the POST cleanup normally performed. This may be helpful during debug. This parameter should normally be left at the default value of 0.

`-ports` *itemlist* Specify a list of user ports to test. By default all the user ports in the current switch will be used. See itemlist for more information.

Example **To run a functional test of all the ports on a switch:**

```
switch:admin> crossporttest -ports 1/0-1/15

Running crossporttest ..............

Ports Segmented (0)
Executing test ...
Test Complete: "crossporttest" Pass 10 of 10
Duration 0 hr, 0 min & 8 sec (0:0:8:725).
 passed.
```

Errors Below are possible error messages if failures are detected:

```
DATA
EPI1_STATUS_ERR
ERR_STAT
ERR_STATS
ERR_STATS_2LONG
ERR_STATS_BADEOF
ERR_STATS_BADOS
ERR_STATS_C3DISC
ERR_STATS_CRC
ERR_STATS_ENCIN
ERR_STATS_ENCOUT
ERR_STATS_TRUNC
ERR_STAT_2LONG
ERR_STAT_BADEOF
ERR_STAT_BADOS
```

```
ERR_STAT_C3DISC
ERR_STAT_CRC
ERR_STAT_ENCIN
ERR_STAT_ENCOUT
ERR_STAT_TRUNC
FDET_PERR
FINISH_MSG_ERR
FTPRT_STATUS_ERR
INIT
LESSN_STATUS_ERR
MBUF_STATE_ERR
MBUF_STATUS_ERR
NO_SEGMENT
PORT_ABSENT
PORT_DIED
PORT_ENABLE
PORT_M2M
PORT_STOPPED
PORT_WRONG
RXQ_FRAME_ERR
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FRX
STATS_FTX
TIMEOUT
XMIT
```

See Also

```
camtest
centralmemorytest
cmemretentiontest
cmitest
itemlist
portloopbacktest
portregtest
spinsilk
sramretentiontest
```

datatypeshow

Displays sample data stream types used in some diagnostic commands.

Syntax `datatypeshow [-seed value]`

Availability All users.

Description Use this command to display sample data stream types used in diagnostic commands. There are 20 different sample data types. The command displays an example of each data stream.

Operands This command has the following operand:

`-seed value` Specify the data pattern seed value. If no seed is specified, then a seed value of 0 is used.

Example **To display sample data streams you can use with diagnostics:**

```
switch:admin> datatypeshow

Pattern         type        example

BYTE_FILL         1     00 00 00 00 00 00 00 00 00 00 00 00
   00 00 00 00
WORD_FILL         2     0000  0000  0000  0000  0000  0000
   0000  0000
QUAD_FILL         3     00000000    00000000    00000000
   00000000
BYTE_NOT          4     00 ff 00 ff 00 ff 00 ff 00 ff 00 ff
   00 ff 00 ff
WORD_NOT          5     0000  ffff  0000  ffff  0000  ffff
   0000  ffff
QUAD_NOT          6     00000000    ffffffff    00000000
   ffffffff
BYTE_RAMP         7     00 01 02 03 04 05 06 07 08 09 0a 0b
   0c 0d 0e 0f
WORD_RAMP         8     0000  0001  0002  0003  0004  0005
   0006  0007
QUAD_RAMP         9     00000000    00000001    00000002
   00000003
BYTE_LFSR        10     69 01 02 05 0b 17 2f 5e bd 7b f6 ec
   d8 b0 60 c0
RANDOM           11     55 16 fc d7 17 65 a9 87 5f 44 be 5a
   d0 de bc a5
CRPAT            12     bc bc 23 47 6b 8f b3 d7 fb 14 36 59
   bc bc 23 47
CSPAT            13     7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e
   7e 7e 7e 7e
CHALF_SQ         14     4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a
   4a 4a 4a 4a
CQTR_SQ          15     78 78 78 78 78 78 78 78 78 78 78 78
   78 78 78 78
RDRAM_PAT        16     00 ff 00 ff 00 ff 00 ff 00 ff 00 ff
   00 ff 00 ff
jCRPAT           17     be d7 23 47 6b 8f b3 14 5e fb 35 59
   be d7 23 47
jCJTPAT          18     7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e 7e
   7e 7e 7e 7e
```

```
jCSPAT          19     7f 7f 7f 7f 7f 7f 7f 7f 7f 7f 7f 7f
   7f 7f 7f 7f
PRED_RAND       20     00000000     11111111     22222222
   33333333

switch:admin>
```

date

Display or set the switch date and time.

Syntax `date ["newdate"]`

Availability All users. (display)

Admin (set)

Description Use this command to set the date and time for a switch (unless security mode is enabled). All switches maintain the current date and time in non-volatile memory. If the Security feature (Secure Mode) is not enabled, switch operation does not depend on the date and time. A switch with incorrect date values continues to function properly. The date and time are only used to recording events in the various logs, for example the error log and the port log.

In order to enable Secure Mode the fabric must be synchronized. Every switch in the fabric must receive a fabric timestamp from the primary FCS switch.

Use this command with no operands to display the local switch date and time. Specify an operand, to set the date and time.

This command sets the a common date and time for the entire fabric. If Secure Mode is not enabled, a change in date or time to one switch is forwarded to the Principal switch and distributed to the fabric. If Secure Mode is enabled, date or time changes can be made only on the Primary FCS switch and distributed to the fabric.

This command becomes read only if external NTP synchronization is enabled. For more information refer to `tsclockserver`.

It may take up to 64 seconds for the switches in the fabric to be synchronized.

The date specified is always the local switch time taking into account daylight saving time and the time zone setup of the switch. Each switch takes care of converting the GMT time distributed fabric-wide to its local time.

The date and time are specified in the following format, as used on many Unix systems:

```
mmddHHMMyy
```

where:

mm is the month, 01-12
dd is the date, 01-31
HH is the hour, 00-23
MM is minutes, 00-59
yy is the year, 00-99

Year values greater than 69 are taken as 1970-1999, year values less than 70 are taken as 2000-2069.

Operands This command has the following operand:

newdate Specify the new date and time in quotation marks. This operand is optional.

Example **To display the current date and time, then modify it:**

```
switch:admin> date
Fri Jan 29 17:01:48 UTC 2000
switch:admin> date "0227123003"
Thu Feb 27 12:30:00 UTC 2003
switch:admin>
```

See Also

```
errlogshow
portlogshow
tsclockserver
tstimezone
uptime
```

dbgshow

Display current values of debug and verbosity levels of the specified module.

Syntax `dbgshow module_name`

Availability All users

Description Use this command to display the current values of debug and verbosity levels of the specified module. If no module name is specified, display debug and verbosity levels of all modules.

Operands This command has the following operands:

module_name Specify the name of the module where you want to view the debug and verbosity levels. Module names are case sensitive. This operand is optional.

Example The following example shows how to use dbgshow to display information about a specific module named NS.

```
switch:admin> dbgshow NS
Module NS,      debug level = 1, verbose level = 1
switch:admin>
```

See Also setdbg

diagclearerror

Dlears the diagnostics failure status.

Syntax diagclearerror [[-slot] *number*] -all

Availability Admin

Description Use this command to clear the diagnostic failure status.

Operands This command has the following operand:

[-slot] *number* Specify the slot to clear the diagnostic failure status. The default is set to 0 and designed to operate on fixed port count products.

-switch *switch* Specify the logical switch number to operate on. If omitted, then all blades will be cleared. This operand is optional.

-all If specified, all blades will be cleared.

If no operand is specified, the default is to clear all bad port flags.

Example **To clear the diag software tag:**

```
switch:admin> diagclearerror 1
 0x1bcb (fabos):  Switch: 0, Error DIAG-CLEARERR, 3,
Pt5 Sl1 Ch0 Qd1 Diagnostics Error Cleared
Err# 0120041 0105
```

diagcommandshow

Displays diagnostic command descriptions.

Syntax `diagcommandshow [command]`

Availability All users

Description Use this command to display a short description of diagnostic commands.

This command may be removed in the future releases. Use diaghelp to lookup diagnostic commands help pages.

Operands This command has the following options:

command	Specify a command name to display more detailed information.

Example **To display a list of diagnostic commands with descriptions:**

```
switch:admin> diagcommandshow
backplanetest - backplane connection test for multi-blade
   systems
backport - test for back-end ASIC pair to ASIC pair
   links.
bladediag - run a suit of diagnostic tests on a switch
   blade
switchdiag - run a suit of diagnostic tests on a switch
   blade
bladediagshort - run a suit of diagnostic tests on a
   switch blade
bladepropshow - display blade properties
burninlevel - set the diagnostics burnin level
burninstatus - display the diagnostics burnin status
camtest - verify QuickLoop's Content Addressable Memory
   CAM) SID translation
centralmemorytest - test ASIC central memory operation
chippropshow - display chip properties
chipregshow - display contents of port registers
cmemretentiontest - data retention test of the central
   mem ory SRAMs
cmitest - verify CMI bus between ASICs
crossporttest - functional test of port external transmit
   and receive path
datatypeshow - display available diagnostic data types
diagclearerror - clears diagnostics failure status
diagcommandshow - display diagnostic command descriptions
diagdisablepost - disable diagnostic POST
```

```
diagenablepost - enable diagnostic POST
diagenv - diagnostic debug parameters management package

---<output truncated>---
```

See Also `diaghelp`

diagdisablepost

Disable POST execution at reboot.

Syntax `diagdisablepost`

Availability Admin

Description Use this command to disable Power On Self Test (POST) execution at switch reboot. This mode is saved in non-volatile memory and POST remains disabled until it is enabled using the `diagenablepost` command. A reboot is not required for this command to take effect.

Brocade recommends that POST always be enabled to ensure the operational status of the switch during the power on stage.

Operands None

Example **To disable the POST during future power ups:**

```
switch:admin> diagdisablepost
Config update Succeeded
Diagnostic POST is now disabled.
switch:admin>
```

See Also `diagenablepost`

diagenablepost

Enable POST execution at next reboot.

Syntax `diagenablepost`

Availability Admin

Description Use this command to enable Power On Self Test (POST) execution at the next switch reboot. This mode is saved in non-volatile memory and POST remains enabled until it is disabled using the

`diagdisablepost` command. A reboot is not required for this command to take effect.

Brocade recommends that POST always be enabled to ensure the operational status of the switch during the power on stage. The factory default enables POST execution.

Operands None

Example **To enable the POST during future power ups:**

```
switch:admin> diagenablepost
Config update Succeeded
Diagnostic POST is now enabled.
switch:admin>
```

See Also `diagdisablepost`

diagesdports

Set ESD skip ports list.

Syntax `diagesdports [itemlist | -show]`

Availability Admin

Description Use this command to set the ESD Idle Ports list. The list is saved in non-volatile memory and stays in that mode until the next execution of `diagesdports`.

The ESD Idle Ports are used by several of the functional test methods to disable testing on the specified list of ports when ESD mode is enabled (see `diagsetesdmode`). The exact type of port list and the exact use of this list are determined by each test method.

The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Operands This command has the following operands:

itemlist	Specify the range of ports to be set to ESD Idle. Refer to `itemlist` for more information.
`-show`	Specify this operand to display ESD Idle Ports list. This operand is optional.

Example **To display the ESD Idle Ports list:**

```
switch:admin> diagesdports -show
ESD Idle Port list is 1-8.
```

See Also

```
diagsetesdmode
itemlist
```

diagfaillimit

Set the diagnostics fail limit to a specified value.

Syntax `diagfaillimit [limit | -show]`

Availability Admin

Description Use this command to set the diagnostics fail limit to a specified value. The fail limit controls the number of failures before certain diagnostics test methods will abort. The normal setting is 1 so that the tests will abort on the first failure. The exact use of this configuration setting depends on the test method.

The fail limit is saved in non-volatile memory and stays set until the next execution of `diagfaillimit`.

The new fail limit becomes active as soon as this command is executed. It does not require a reboot to take effect.

Operands This command has the following operands:

limit	Specify the number of failures before a diagnostic test aborts. The limit value must be 1 or greater. This operand is optional.
-show	Specify this operand to display the current fail limit setting. This operand is optional.

If no operand is specified the current value is displayed.

Example **To change the fail limit from 1 to 5:**

```
switch:admin> diagfaillimit -show
Fail Limit is 1.
switch:admin> diagfaillimit 5
Fail Limit is now 5.
Config update Succeeded
switch:admin>
```

diaghelp

Display diagnostic command information.

Syntax `diaghelp [-name command]`

Availability All users

Description Use this command to display a short description of diagnostic commands.

Operands This command has the following operand:

`-name command` Specify a command name to display more detailed information. This will display a parameter list, subtest information, and diagnostic error codes if available.

Example **To display information about diagnostic commands:**

```
switch:admin> diaghelp
backplanetest - backplane connection test for multi-blade
   systems
backport - test for back-end ASIC pair to ASIC pair
   links.
bladediag - run a suit of diagnostic tests on a switch
   blade
switchdiag - run a suit of diagnostic tests on a switch
   blade
bladediagshort - run a suit of diagnostic tests on a
   switch blade
bladepropshow - display blade properties
burninlevel - set the diagnostics burnin level
burninstatus - display the diagnostics burnin status
camtest - verify QuickLoop's Content Addressable Memory
   CAM) SID translation
centralmemorytest - test ASIC central memory operation
chippropshow - display chip properties
chipregshow - display contents of port registers
cmemretentiontest - data retention test of the central
   mem ory SRAMs
cmitest - verify CMI bus between ASICs
crossporttest - functional test of port external transmit
   and receive path
datatypeshow - display available diagnostic data types
diagclearerror - clears diagnostics failure status
diagcommandshow - display diagnostic command descriptions
diagdisablepost - disable diagnostic POST
diagenablepost - enable diagnostic POST
diagenv - diagnostic debug parameters management package
```

```
diagesdports - set ESD skip ports list
diagfaillimit - set diagnostics fail limit
diaghelp - display diagnostic command descriptions
diagloopid - select the diagnostics loop ID
diagmodepr - set or display diagnostic print mode
diagmodeshow - display diagnostic mode configuration
diagpost - set or display diagnostic POST configuration
diagretry - set or display diagnostic retry mode
diagsetburnin - initializes the blade for a burnin run.
diagsetcycle - set diagnostic script parameters
diagshow - display diagnostics status
diagshowtime - set or display diagnostic show-time mode
diagsetshowtime - set or display diagnostic show-time
   mode
diagsilkworm - set or display silkworm mode
diagskiptests - set or display diagnostics skip test
   flags
diagstatus - display currently running diagnostic tests
diagstopburnin - terminate burnin run on a blade
filtertest - frame filter test for bloom ASICs
itemlist - List parameter syntax and grammar information.
loopporttest - functional test of L-port M->M path on a
   loop
minicycle - functional test of internal and external
   trans mit and receive pa
ths at full speed
mulregdump - display the contents of port registers and
   mem ories
portledtest - cycle user port LEDs
portloopbacktest - functional test of port N->N path
portregtest - write/read test of the ASIC SRAMs &
   registers
porttest - functional test on a live fabric. Starts
   porttest.
porttestshow - retreive information from porttest.
ptbufshow - dump port buffer contents
ptcreditshow - display port credits
ptdatashow - display port data structures
ptphantomshow - display the quick-loop CAM tables
ptpropshow - display port property contents
ptregshow - display contents of port registers
ptrouteshow - display port routing tables
ptstatsshow - display port statistics
ramdump - display the contents of port internal registers
setesdmode - set or display ESD mode
diagsetesdmode - set or display ESD mode
setmediamode - set or display media mode
setsfpmode - set or display media mode
setgbicmode - set or display media mode
setmfgmode - set or display diagnostic MFG mode
setsplbmode - set or display SPLB mode
```

```
spinfab - functional test of switch to switch ISL cabling
   and trunk group operation
spinjitter - line-speed jitter measurement
spinsilk - functional test of internal and external
   transmit and receive paths at full speed
sramretentiontest - data retention test of the
   miscellaneous SRAMs in ASIC
statsclear - clear port and diagnostic statistics
statstest - statistics counter test for bloom ASICs
stopporttest - terminate the running porttest
supportshow - configurable groups of predefined dis play
   commands for debugging
supportshowcfgshow - configurable groups of predefined
   dis play commands for debugging
supportshowcfgenable - configurable groups of predefined
   dis play commands for debugging
supportshowcfgdisable - configurable groups of predefined
   dis play commands for debugging
systemtest - run a series of diagnostic tests on a switch
   blade
systemverification - run a suit of diagnostic tests on
   all switches in a system
turboramtest - turbo SRAM test for bloom ASICs
txdpath - functional test of ASIC pair TXA TXD
   connections
voltagemargin - set the slot voltage margin
switch:admin>
```

diagloopid

Set the diagnostics loop ID.

Syntax `diagloopid [id | -show]`

Availability Admin

Description Use this command to select the loop ID to be used by FL mode diagnostics. The value entered will be converted from a loop ID to the corresponding ALPA and used as the port address for any diagnostics that operate in FL port mode.

The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Operands This command has the following operands:

id	Specify the loop Id for FL mode diagnostics. This operand is optional.

`-show` Specify `-show` to display the current loop ID. This operand is optional.

If no operand is specified the current value is displayed.

Example **To display the Loop ID:**

```
switch:admin> diagloopid
FL mode Loop ID is 125.
switch:admin>
```

Currently no FL mode tests exist.

diagmodepr

Enable or disable mode messages.

Syntax `diagmodepr [mode | -show]`

Availability Admin

Description Use this command to enable print mode (specify value of 1) or disable print mode (specify value of 0). The mode is saved in non-volatile memory and stays in that mode until the next execution of `diagmodepr`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Print mode when enabled will cause extra messages to be displayed in the burn-in and POST scripts. The exact behavior varies depending on the script being run.

Operands This command has the following operands:

mode Specify 1 to enable print mode, specify 0 to disable print mode. This operand is optional.

`-show` Specify this operand to display the current mode. This operand is optional.

If no operand is specified the current value is displayed.

Example **To enable print mode messages:**

```
switch:admin> diagmodepr -show
Diagnostic Print Mode is currently disabled.
switch:admin> diagmodepr 1
Config update Succeeded
```

```
Diagnostic Print Mode is now enabled.
switch:admin>
```

diagpost

Set or display diagnostic POST configuration.

Syntax `diagpost [mode | -show]`

Availability Admin

Description Use this command to enable or disable POST testing. The mode is saved in non-volatile memory and stays in that mode until the next execution of `diagpost`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Post mode modifies the behavior of the diagnostics daemon program to inhibit testing of switch blades when the system is first powered on or a new blade is added.

Operands This command has the following operands:

mode	Specify 1 to enable POST test, specify 0 to disable POST test. This operand is optional.
`-show`	Specify this operand to display the current mode. This operand is optional.

If no operand is specified the current value is displayed.

Example **To enable and then disable the POST test:**

```
switch:admin> diagpost
Diagnostic POST is currently disabled.
switch:admin> diagpost 1
Config update Succeeded
Diagnostic POST is now enabled.
switch:admin>
```

See Also

```
diagdisablepost
diagenablepost
```

To enable or disable diagnostic POST, the recommended method is to use `diagenablepost` and `diagdisablepost`.

---

diagretry

Set or display diagnostic retry mode.

Syntax `diagretry [mode | -show]`

Availability Admin

Description Use this command to enable retry mode if mode value is non-zero and disable the retry mode if mode value is 0. The mode is saved in flash memory and stays in that mode until the next execution of diagretry. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Retry mode when enabled modifies the behavior of the diagnostic test methods, POST (Power-On Self-Test), and burnin scripts. The exact behavior depends on the tests and scripts that are run.

Operands This command has the following operands:

mode	Specify 1 to enable retry mode, specify 0 to disable retry mode. This operand is optional.
`-show`	Specify this operand to display the current mode setting. This operand is optional.

If no operand is specified the current value is displayed.

Example **To view the current retry mode value:**

```
switch:admin> diagretry -show
Diagnostic Retry Mode is currently enabled.
switch:admin>
```

diagsetburnin

Initializes the blade for a burnin run.

Syntax `diagsetburnin [--slot number] [script | -current]`

Availability Admin

Description This sets up the blade burnin parameters for the registered burnin script. The name of burnin script can be set with `burninname`

command alternatively. The burnin will start at the next run of POST (Power-On Self-Test) on the designated blade(s).

The errors and activity logs are stored in non-volatile memory. The activity log of the script is saved in `/var/log/scriptname.slot.log`. The errors produced are available from `burninerrshow` command on a per blade basis. When power cycles occur, the burnin activity is restarted at the test that was interrupted at the time of the power cycle. This command does not require a reboot to take effect.

Options

This command has the following operands:

`-slot` *number*	Specify which slot number to update. If this option is not specified at all, then all slots on the switch are setup for burnin.
script	Specify the name of the burnin script to run.
`-current`	Set the name of burnin script to current burnin script.

Examples

To set the burnin script and mode:

```
switch:admin> diagsetburnin --slot 1 -current
existing script is: /fabos/share/switchess.sh
Burnin mode is Enabled.
Removing all log files in /var/log for slot 1
Slot 1 burnin name is now /fabos/share/switchess.sh
Config update Succeeded
```

See Also

`burninerrshow`
`burninname`
`diagsetcycle`

Boards must be installed prior to running this command and `diagsetcycle` must be run prior to `diagsetburnin` if you wish to use both commands.

---

diagsetcycle

Set diagnostic script parameters.

Syntax `diagsetcycle` *`script`* `[-show | -default | [-keyword` *`value`*`]]`

Availability Admin

Description This command provides an interactive method to update diagnostic command parameters. If only a script is specified, it will display all configuration variables used by the specified script and enter an interactive session. Using the full parameters, variables can be updated non-interactively.

In interactive mode, the current value, default value, and description of purpose of the variable are displayed for each variable. If no new value is specified, then the current value is left unchanged. If a new value is entered, then its value is updated, and stored in the configuration database for that blade type. This command does not require a reboot to take effect.

Options This command has the following operands:

`script`	Specify a script where you want to change parameters.
`-show`	Specify this operand to display the parameters for the specified diagnostic *script*.
`-default`	Specify this operand to set the script parameters to default values.
`-keyword` *`value`*	The script parameters can be updated non-interactively using this style of option list. keyword is the keyword to update and the value should be specified manually in this case

Examples **To update diagnostic command parameters:**

```
switch:admin> diagsetcycle switchburnin.sh -show
CURRENT - KEYWORD          : DEFAULT
 1      - number_of_runs   : 1
 2      - vib              : 2
 10     - thermal          : 10
 BURNIN - label            : BURNIN
 1      - tbr_passes       : 1
 1      - prt_on           : 1
 1      - cntmem_on        : 1
```

```
1       - cmi_on          : 1
1       - retention_on    : 1
1       - cam_on          : 1
50      - flt_passes      : 50
25      - sta_passes      : 25
100     - plb_nframes     : 100
50      - txd_nframes     : 50
200     - xpt_nframes     : 200
20      - bpt_nframes     : 20
50      - slk_nmegs       : 50
30      - bpt_all_nframes: 30
50      - slk_all_nmegs   : 50
```

See Also

```
burninname
burninlevel
burninscript
diagsetburnin
diagstopburnin
```

diagshow

Display diagnostics status.

Syntax `diagshow [--slot number] [-uports itemlist] [-bports itemlist] [-use_bports value]`

Availability All users

Description Use this command to display the diagnostics status for the specified list of blade or user ports.

Options This command has the following options:

`-slot number` Specify which slot to operate on. If this option is not specified, the default slot will be assumed. The default slot is 0 and designed to operate on fixed port count products. By default this command displays all user ports in the system.

`-uports itemlist` Specify a list of user ports to display. This operand is optional.

`-bports itemlist` Specify a list of blade ports to display. This operand is optional.

`-use_bports value`
: If value is set to non-zero, then the diagnostics status for the blade ports specified in `-use_bports` will be displayed, otherwise the user ports specified in `-uports` is displayed. The default value is 0. This operand is optional.

Example **To display diagnostic status on a switch blade:**

```
switch:admin> diagshow
Diagnostics Status:  Fri Feb 08 15:25:24 2002
Slot: 1 UPORTS
Port      BPort     Diag      Active    Speed      ......
 0         15        OK          UP      2G Auto    ......
 1         14        OK          UP      2G Auto    ......
 2         13        OK          UP      2G Auto    ......
 3         12        OK          UP      2G Auto    ......
 4         31        OK          UP      2G Auto    ......
 5         30        OK          UP      2G Auto    ......
 6         29        OK          UP      2G Auto    ......
 7         28        OK          UP      2G Auto    ......
 8         47        OK          UP      2G Auto    ......
--- <output truncated> ---
```

See Also `itemlist`

diagshowtime

Set or display diagnostic show-time mode.

Syntax `diagshowtime [mode | -show]`

Availability Admin

Description Use this command to enable show-time mode (if the mode value is set to a non-zero value) or disable the show-time mode (if the mode value is set to 0). The mode is saved in flash memory and stays in that mode until the next execution of `diagshowtime`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Show-time mode when enabled causes each test to display elapsed time messages. It is normally used during burnin and for test method debugging.

Options This command has the following options:

mode	Specify 1 (or any non-zero value) to enable show time mode, specify 0 to disable show-time mode. This operand is optional.
-show	Specify this operand to display the current mode setting. This operand is optional.

If no operand is specified the current value is displayed.

Example

To enable show time mode:

```
switch:admin> diagshowtime
Show Time mode is 0 (Disabled).
switch:admin> diagshowtime 1
Config update Succeeded
Show Time mode is now 1 (Enabled).
switch:admin>
```

`diagsetshowtime` is an alias of `diagshowtime`.

---

diagsilkworm

Enable or disable silkworm mode.

Syntax `diagsilkworm [mode | -show]`

Availability Admin

Description Use this command to enable silkworm mode (if the mode value is set to a non-zero value) or disable the silkworm mode (if the mode value is set to 0). The mode is saved in flash memory and stays in that mode until the next execution of diagsilkworm. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Silkworm mode when enabled notifies the diagnostics environment and test methods that the tests are running in silkworm mode. For proper operation FCSW mode must also be disabled

Operands This command has the following operands:

mode	Specify 1 to enable silkworm mode, specify 0 to disable silkworm mode. This operand is optional.
-show	Specify this operand to display the current mode setting. This operand is optional.

If no operand is specified the current value is displayed.

Example **To enable silkworm mode:**

```
switch:admin> diagsilkworm -show
Silkworm mode is 0 (Disabled).
```

This mode may not be used by burnin or POST scripts for multi-blade systems because it is a switch-wide configuration.

diagskiptests

Enable or disable diagnostics skip test flags.

Syntax `diagskiptests [value | -show]`

Availability Admin

Description Use this command to enable or disable the diagnostics skip test flags. The skip test flags are saved in non-volatile memory and stay set until the next execution of `diagskiptests`.

The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

The skip test flags are used to skip the execution of certain POST tests that may prove hazardous to normal switch operation. The exact use of this flag is determined by the post scripts and the specific test methods that are used.

Operands This command has the following operands:

value	Specify a bit mask for tests to be skipped.
-show	If specified or no value is given, the current skip test flags will be displayed.

If no operand is specified the current value is displayed.

Example The following is an example of the diagskiptests command:

```
switch:admin> diagskiptests -show
Skip tests is 0.
switch:admin> diagskiptests 1
Config update Succeeded
Skip tests is now 1.
switch:admin>
```

diagstopburnin

Terminate a blade burn-in run.

Syntax `diagstopburnin [--slot number]`

Availability Admin

Description Use this command to determine which PID is running burn-in on a blade and terminate that activity. It is expected that the burn-in script handles the logging cleanup.

This command does not require a reboot to take effect.

Operands This command has the following operands:

`-slot number` Specify the slot to stop burn-in. If no slot is specified this command executes on all slots in the logical switch. This operand is optional.

Example **To stop burn-in mode on a switch:**

```
switch:admin> diagstopburnin --slot 1
No burnin script active on slot 1
 1 burninErrShow output:
0x1eea (fabos): Dec 19 14:42:18
Switch: 0, Error DIAG-MANUAL1, 1, " 1 Starting switchess
   ...
Err# 0140042 0100:101:000:001:24:37:

0xc84 (fabos): Dec 20 08:57:27
Switch: 0, Error DIAG-MANUAL1, 1, " 1 switchess: ABORT
   ...
Err# 0140042 0100:101:000:000:25:41:

0x1b61 (fabos): Feb 07 19:02:28
Switch: 0, Error DIAG-MANUAL1, 1, " 1 Starting switchess
   ...
Err# 0140042 0100:101:000:001:26:39:

0x47ff (fabos): Feb 07 21:45:36
Switch: 0, Error DIAG-MANUAL1, 1, " 1 switchess: ABORT
   ...
Err# 0140042 0100:101:000:002:26:41:1N
switch:admin>
```

See Also `diagsetburnin`

dlsreset

Disable Dynamic Load Sharing (DLS) option.

Syntax `dlsreset`

Availability Admin

Description Use this command to turn off DLS when a fabric change occurs. Refer to `dlsset` for a full description of load sharing.

This command should be used only if devices connected to the fabric can not handle occasional routing changes correctly.

Operands None

Examples **To disable the dynamic load sharing option:**

```
switch:admin> dlsreset
Committing configuration...done.
switch:admin> dlsshow
DLS is not set
```

See Also

```
dlsset
dlsshow
```

dlsset

Enable Dynamic Load Sharing (DLS) option.

Syntax `dlsset`

Availability Admin

Description Use this command to turn on DLS when a fabric change occurs.

Routing is generally based on the incoming port and the destination domain. This means that all the traffic coming in from a port (either E_Port or Fx_Port) directed to the same remote domain is routed through the same output E_Port.

To optimize fabric routing, when there are multiple equivalent paths to a remote switch, traffic is shared among all the paths. Load sharing is recomputed when a switch is booted up or every time a change in

the fabric occurs. A change in the fabric is defined as an E_Port going up or down, or an Fx_Port going up or down.

If DLS is turned off (using `dlsreset`), load sharing is performed only at boot time or when an Fx_Port comes up. Optimal load sharing is rarely achieved with DLS disabled.

If DLS is turned on (using `dlsset`), routing changes can affect working ports. For example, if an Fx_Port goes down, another Fx_Port may be rerouted from one E_Port to a different E_Port. The switch minimizes the number of routing changes, but some are necessary in order to achieve optimal load sharing.

Operands None

Examples **To enable the dynamic load sharing option:**

```
switch:admin> dlsset
Committing configuration...done.
switch:admin> dlsshow
DLS is set
```

See Also

```
dlsreset
dlsshow
iodset
iodreset
iodshow
urouteshow
topologyshow
```

dlsshow

Display the setting of the Dynamic Load Sharing (DLS) option.

Syntax `dlsshow`

Availability All users

Description Use this command to display whether DLS is on or off. There can be two messages displayed:

`DLS is set` The DLS option is turned on. Load sharing is reconfigured with every change in the fabric.

`DLS is not set` The DLS option is turned off. Load sharing is only reconfigured when the switch is rebooted or an Fx_Port comes up.

Operands None

Example To display the current DLS option setting:

```
switch:admin> dlsshow
DLS is set
```

See Also

```
dlsset
dlsreset
```

dnsconfig

Set or display Domain name service parameters.

Syntax

```
dnsconfig
```

Availability Admin

Description Use this command to display or set the domain name service parameters.

The domain name service parameters are namely domain name and the name server IP address for primary and secondary name servers.

Operands None

Example **To set the DNS parameters for the system:**

```
switch:admin> dnsconfig

Enter option
1 Display Domain Name Service (DNS) configuration
2 Set DNS configuration
3 Remove DNS configuration
4 Quit
Select an item: (1..4) [4] 2

Enter Domain Name: [] domain.com
Enter Name Server IP address in dot notation: []
   123.123.123.123
Enter Name Server IP address in dot notation: []
   123.123.123.124
DNS parameters saved successfully

Enter option
1 Display Domain Name Service (DNS) configuration
2 Set DNS configuration
3 Remove DNS configuration
4 Quit
```


```
Select an item: (1..4) [4] 4
switch:admin>
```

See Also

```
ipaddrshow
ipaddrset
```

errclear

Clear the switch error log.

Syntax

```
errclear [-p]
```

Availability

Admin

Description

Use this command to clear the error log for a particular switch instance. If no operand is specified, this command clears the error log in RAM; The persistent error log is not cleared. However, if `-p` option is specified, *only* the persistent error log is cleared and the error log in RAM is not cleared.

When the error log in RAM is cleared, `errshow` and `errdump` no longer show the persistent error logs unless the `-p` parameter is used.

Operands

This command has the following operands:

`-p`	Clear messages *only* from the persistent error log. Error log in RAM is not cleared.

Example

The following example shows how to clear the current run time error log on the Active CP.

```
switch:admin> errclear
```

The following example shows how to clear the persistent error log on the Active CP.

```
switch:admin> errclear -p
```

See Also

```
errdump
errshow
errnvlogsizeset
errnvlogsizeshow
```

errdump

Display the error log, without page breaks.

Syntax `errdump [-a] [-p]`

Availability Admin

Description Use this command to display the error log, showing entries in the log without any page breaks. It is identical to `errshow`, except that `errshow` prompts the user to type return between each log entry.

The output of the `errdump` command includes the display of errors/events history recorded in the persistent error log and error/events logged in the current run time cycle. This command also provides options to display *only* those error/event messages that are saved in the persistent error log, or *only* those messages generated during the current run time cycle.

All important error log messages, regardless of their message severity level, are stored in a persistent storage as they are logged. Both the persistent error log and the run time log are limited in space and managed as circular buffers. When either log overflows, old entries are replaced by new entries.

The persistent error log is saved across system reboots and power cycles and can be resized at run time.

Error log messages are not persistent across failovers. Messages saved to the persistent error log are saved to the active CP. CP0 and CP1 have different persistent error logs, and the errshow and errdump command output is different depending on the CP you log into.

Operands This command has the following operands:

`-a`	Display messages from the active error log. This displays the error log messages generated during the current run time cycle.
`-p`	Display messages from the persistent error log.

Example **To display the error log without page breaks:**

```
switch:admin> errdump

Error 03
--------
```


```
0x2a5 (fabos): Jun 14 12:03:51
Switch: 0, Debug HAMKERNEL-IP_UP, 5, (session=3)
   Heartbeat up from Standby CP

Error 02
--------
0x2a5 (fabos): Jun 14 12:03:50
Switch: 0, Info HAM-REDUNDANT_INFO, 4,
(Heartbeat Up) System in REDUNDANT state

Error 01
--------
0x28b (fabos): Jun 14 12:01:27
Switch: 0, Error EM-CP_ERR, 2, CP in slot 5 set to faulty
   because of CP ERROR

switch:admin>
```

See Also

```
errshow
errsavelvlset
errsavelvlshow
errnvlogsizeset
errnvlogsizeshow
```

errnvlogsizeset

Resize the persistent error log.

Syntax `errnvlogsizeset` *`number_of_entries`*

Availability Admin

Description Use this command to resize the persistent error log of a switch to a new size specified by the operand *`number_of_entries`*. The persistent error log is resized immediately after the successful execution of this command.

Operands This command has the following operands:

`number_of_entries`
: Specify the new persistent error log size in unit of number of error log entries. The error log can be resized within the specified limits. This command fails if an attempt is made to change the persistent error log beyond the range of valid values. Valid values are from 1024 to 2048.

Example The following example shows how to resize the persistent error log to 1500 entries.

```
switch:admin> errnvlogsizeset 1500

Persistent error log is  resized to store 1500 entries

switch:admin>
```

See Also
```
errnvlogsizeshow
errsavelvlshow
errshow
```

errnvlogsizeshow

Display the current persistent (non-volatile) error log configuration of a switch.

Syntax `errnvlogsizeshow`

Availability All users

Description Use this command to show the current maximum size of the persistent error log.

The configuration of the persistent error log on the active CP is independent of the configuration on the standby CP.

Operands None

Example The following example shows how to display persistent error log configuration.

```
switch:admin> errnvlogsizeshow

Persistent Error Log can store  1024 entries

switch:admin>
```

See Also
```
errnvlogsizeset
errsavelvlshow
errshow
```

errsavelvlset

Set error save level of a switch.

Syntax `errsavelvlset lvl`

Availability Admin

Description Use this command to control types of messages that are saved in the persistent error log. Message types are based on the message severity levels. By default, all messages of type Panic and Critical are saved in the persistent log. If you want to save messages of log levels less severe than Critical, use this command to specify a new message save level. This new message save level is not persistent across a reboot. It is in effect only for that run time cycle.

Operands This command has the following operands:

lvl	Message severity level. Save those error log messages whose message severity level is less than (more severe) or equal to this level. The valid values are: Critical 1 Error 2 Warning 3 Info 4 Debug 5

Example The following example shows how to enable saving of Warning, Error, Critical and Panic messages in the persistent error log

```
switch:admin> errsavelvlset 3
switch:admin>
```

See Also
`errdump`
`errsavelvlset`
`errsavelvlshow`
`errnvlogsizeset`

errsavelvlshow

Display the current error save level setting of a switch.

Syntax `errsavelvlshow`

Availability Admin

Description Use this command to find out the current value of the persistent error log save level for a given switch instance.

Operands None

Example Following example shows how to display current error log save level.

```
switch:admin> errsavelvlshow

 Current message save level is = 1

switch:admin>
```

See Also

```
errsavelvlset
errnvlogsizeset
errnvlogsizeshow
errshow
```

errshow

Display the error log.

Syntax `errshow [-a] [-p]`

Availability All users

Description Use this command to display the error log, prompting the user to type return between each log entry. It is identical to errDump, except that errDump displays all entries without page breaks. The output of errshow command includes the display of errors/events recorded in the persistent error log during previous run time cycles and the display of error/event messages logged in the current run time cycle.

This command also provides options to display *only* those error log messages that are saved in the persistent log and to display *only* those messages that are logged during the current run time cycle.

All important error log messages, regardless of their message severity level, are stored in a persistent storage as they are logged. Both the persistent error log and the run time log are limited in space and managed as circular buffers. When either log overflows, old entries are replaced by new entries.

The persistent error log is saved across system reboots and power cycles and can be resized at run time.

Error log messages are not persistent across failovers. Messages saved to the persistent error log are saved to the active CP. CP0 and CP1 have different persistent error logs, and the errshow and errdump command output is different depending on the CP you log into.

Operands

This command has the following operands:

`-a`	Display messages from the active error log. This displays the error log messages generated during the current run time cycle.
`-p`	Display messages from the persistent error log.

Example

To display the error log with page breaks:

```
switch:admin> errshow

Error 14
--------
0x304 (fabos): Jun 14 11:57:52
Switch: 0, Warning FW-STATUS_SWITCH, 3, Switch status
   changed from HEALTHY/OK to
 Marginal/Warning

Type <CR> to continue, Q<CR> to stop:
```

See Also

```
errdump
errsavelvlset
errsavelvlshow
errnvlogsizeset
errnvlogsizeshow
```

exit

Logout from a shell session.

Syntax `exit`

Availability All users

Description Use this command to logout from a telnet, rlogin or serial port session. Telnet and rlogin connections are closed, the serial port returns to the `login:` prompt.

The commands `exit` and `quit` are accepted as synonyms for logout, as is a Control-D typed at the beginning of a line.

Operands None

Example **To exit from a shell session:**

```
switch:admin> exit
Connection to host lost.
```

See Also `logout`

fabportshow

Display fabric port information.

Syntax `fabportshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display the contents of a particular port data and also any pending commands (if applicable). The following information is displayed:

Port	Displays the port number.
State	The state of the port: P0 - Port Offline P1 - Port Online P2 - ELP ACC Received P3 - Link Reset Done I0 - Trunk Initiator: EMT Sent I1 - Trunk Initiator: ETP ACC Received I2 - Trunk Initiator: ETP Sent

I3 - Trunk Initiator: Link Reset
T0 - Trunk Target: EMT Received
T1 - Trunk Target: ETP Received
T2 - Trunk Target: Link Reset

List — IU list pointer.

Flags — Port flags:

0x00000001	slave connection
0x00000002	loop back connection
0x00000004	incompatible connection
0x00000008	overlapping domains
0x00000010	overlapping zones
0x00000020	done PTIO ioctl
0x00000040	sent a RJT to ELP
0x00000080	BF received from the port
0x00000200	segmented by routing code
0x00000800	zoning has completed
0x00001000	segmented by Platform Management
0x00002000	segmented due to no license
0x00004000	segmented due to E_Port disabling
0x00008000	DIA already sent for that port
0x00010000	RDI already sent
0x00020000	port is true T port
0x00040000	Port received an ELP
0x00080000	Port received an ELP RJT
0x00100000	LR Pending due to ELP RJT rcv
0x00200000	Received a DIA on this port
0x00400000	Port is the EMT Initiator
0x00800000	Security violation
0x01000000	Security incompatibility
0x02000000	Rcv a DIA ACC

nbrWWN — Neighboring switch's WWN

red_ports — All E-Ports that are connected to the same neighboring switch.

Operands

This command has the following operands:

slotnumber — Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port

number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display fabric port information:**

```
switch:admin> fabportshow 4/14
Fabric Port Information:
========================

Port:         62
State:        P3
List:         0x10068418
List Count:   0
Flags:        0x280120
nbrWWN:       10:00:00:60:69:80:06:cf
red_ports:
10 11 62 63

Open commands pending:
======================
No commands pending

switch:admin>
```

See Also portshow

fabretryshow

Display the retry count of the fabric commands.

Syntax `fabretryshow`

Availability All users

Description Use this command to display the retry count of the fabric commands. The first line of display shows:

SW_ISLISL ports

Each line below shows the retry count for the following fabric commands:

- ELPExchange Link Parameters
- EFPExchange Fabric Parameters
- DIADomain Identifier Assigned
- RDIRequest Domain Identifier
- BFBuild Fabric
- RSCNRemote State Change Notification
- FWDFabric Controller Forward
- EMTFabric Controller Mark Timestamp
- GAIDGet Address IDentifier
- INQInquiry command

Operands None

Example **To display the retry count of Fabric OS commands:**

```
switch:user> fabretryshow
                          E_Ports
SW_ILS          45        51       59

ELP             0         0        0
EFP             0         0        0
DIA             0         0        0
RDI             0         0        0
BF              0         0        0
RSCN            0         0        0
FWD             0         0        0
EMT             0         0        0
ETP             0         0        0
```

RAIT	0	0	0
GAID	0	0	0
INQ	0	0	0
	0	0	0
	0	0	0
	0	0	0
	0	0	0

See Also

`fabstatsshow`

fabricprincipal

Set the Principal Switch Selection mode.

Syntax

`fabricprincipal [-fhq] [ 1 | 0 ]`

Availability

All users can display current setting.

Admin can modify current setting.

Description

Use this command to set Principal Switch Selection Mode for the switch.

The implementation of the `fabricprincipal` command is based solely on mechanisms specified in the Fibre Channel standards. These mechanisms provide a *preference* for a switch requesting to be the principal switch in a fabric, but they do not provide an absolute guarantee that a switch requesting to be the principal switch will actually achieve this status.

When dealing with larger fabrics, the selection of the principal switch is less deterministic. In these cases, to help ensure that the desired switch is selected as the principal switch, a small selection of switches should be connected together first, followed by the addition of the rest of the fabric.

Operands

This command has the following operands:

`-f` Specify the `-f` option to force a fabric rebuild. This option is required with when enabling principal switch mode.

`-h` Specify the `-h` option to display out command usage summary.

`-q` Specify the `-q` option to display the current mode state.

`1 | 0`	Specify 1 to enable principal switch mode, or specify 0 to disable principal switch mode (the mode activates when the fabric rebuilds). This operand is optional.

Example

To display the current mode setting:

```
switch:admin> fabricprincipal -q
Principal Selection Mode: Enable
```

To disable the mode setting:

```
switch:admin> fabricprincipal 0
Principal Selection Mode disabled
```

To enable the mode setting:

```
switch:admin> fabricprincipal 1
Principal Selection Mode enabled
```

To enable the mode setting and force fabric rebuild:

```
switch:admin> fabricprincipal -f 1
Principal Selection Mode enabled (Forcing fabric rebuild)
```

See Also `fabricshow`

fabricshow

Display fabric membership information.

Syntax `fabricshow`

Availability All users

Description Use this command to display information about switches and multicast alias groups in the fabric.

If the switch is initializing, or disabled, the message `no fabric` is displayed. If the fabric is reconfiguring, some or all switches may not be shown. Otherwise, the following fields are shown:

Switch ID	The switch `Domain_ID` and embedded port `D_ID`.
Worldwide Name	The switch WWN.
Enet IP Addr	The switch ethernet IP address.
FC IP Addr	The switch FC IP address.

Name	The switch symbolic name. An arrow (>) indicates the principal switch.

Multicast alias groups are created on demand by request from N_Ports attached to the alias server; typically no groups are listed. If multicast alias groups exist, the following information is shown:

Group ID	The alias group number and D_ID.
Token	The alias group token (assigned by the N_Port).

Operands None

Example The following example shows a fabric of four switches. `sw180` is the principal switch. Three of the switches are configured to run IP over fibre channel. There is one multicast alias group.

```
switch:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr       Name
-------------------------------------------------------------------------
3: fffc43 10:00:00:60:69:10:60:1f  192.168.64.187  0.0.0.0          "sw187"
2: fffc42 10:00:00:60:69:00:05:91  192.168.64.60   192.168.65.60    "sw60"
1: fffc41 10:00:00:60:69:00:02:0b  192.168.64.180  192.168.65.180  >"sw180"
0: fffc40 10:00:00:60:69:00:06:56  192.168.64.59   192.168.65.59    "sw5"
The Fabric has 4 switches
Group ID    Token
-----------------
0: fffb01 40:05:00:00:10:00:00:60:69:00:00:15
```

See Also `switchshow`

fabstateclear

Clears the fabric state information.

Syntax fabstateclear

Availability Admin

Description Use this command to clear the queue of fabric state information logged by the fabric.

Operands None

Example **To clear the fabric state information:**

```
switch:admin> fabstateclear
switch:admin> fabstateshow
Time Stamp   Input and *Action                            S, P   Sn,Pn  Port  Xid
=============================================================================
switch:admin>
```

See Also fabstateshow

fabstateshow

Display the fabric state information.

Syntax fabstateshow

Availability All users

Description Use this command to display the queue of fabric state information logged by the fabric.

Operands None

Example To display the fabric state information:

```
switch:admin> fabstateshow
Time Stamp   Input and *Action                             S, P    Sn,Pn  Port  Xid
===========================================================================
10:58:35.185 BF Rcv                                      A2,P3   A2,P3   4     0x287
10:58:35.185 *Change State                                 A2,NA   F0,NA  NA     NA
10:58:35.185 BF sending ACC                               F0,P3   F0,P3   4     0x287
10:58:35.197 *Canceling All Node Timers                    F0,NA   F0,NA  NA     NA
10:58:35.198 *BF Flood                                     F0,NA   F0,NA  NA     NA
10:58:35.200 *BF Send                                    F0,P3   F0,P3  40     0x253
10:58:35.200 *BF Flood Done                                F0,NA   F0,NA  NA     NA
10:58:35.200 *Cancel 2 * F_S_TOV Timer                     F0,NA   F0,NA  NA     NA
10:58:35.204 *Cancel EFP Flood Timer                       F0,NA   F0,NA  NA     NA
10:58:35.204 *Cancel RDI Receive Timer                     F0,NA   F0,NA  NA     NA
10:58:35.205 *Cancel RDI Send  Timer                       F0,NA   F0,NA  NA     NA
10:58:35.205 *Start F_S_TOV Timer                          F0,NA   F0,NA  NA     NA
```

See Also fabstateclear
fabportshow

fabstatsshow

Display the fabric statistics information.

Syntax `fabstatsshow`

Availability All users

Description Use this command to display the statistics information of fabric. The information displayed is as follows:

- Number of times a switch domain ID has been forcibly changed
- Number of E_Port offline transitions
- Number of fabric reconfigurations
- Number of fabric segmentations due to:

  Loopback
  Incompatibility
  Overlap
  Zoning
  Routing
  Licensing
  Disabling E_Port

Operand None

Example **To display the fabric statistics information:**

```
switch:admin> fabstatsshow
Description                          Count
-----------------------------------------
Domain ID forcibly changed:              2
E_Port offline transitions:              0
Reconfigurations:                        9
Segmentations due to:
                    Loopback:            0
              Incompatibility:           0
                     Overlap:            0
                      Zoning:            2
                     Routing:            2
                   Licensing:            4
            Disabling E_Port:            0
switch:admin>
```

See Also `fabretryshow`

fabswitchshow

Display the fabric switch state structure information.

Syntax `fabswitchshow`

Availability All users

Description Use this command to display the fabric switch state structure information. This command is strictly for debugging purpose. It is not intended as a user command.

Operands None

Example To display fabric switch state structure:

```
switch:admin> fabswitchshow
Fabric Switch State Structure Information
=========================================
State:                    A2
Rdi Receive Timer:        0x10051b48, IDLE STATE
Unconfirmed Sw Timer:     0x10051c50, IDLE STATE
Principal Domain:         4
Upstream Port:            4
Principal Wwn:            10:00:00:60:69:00:54:e8
Principal Prioritry:      0x2
Flags:                    0x8
inq_sem count:            1
dbg_sem count:            1
fab_q current count:      0
fab_q high water:         16
fab_q age:                0 (sec)
dup xid occurance:        0
last message:
14:47:57.029 RSCN Rcv addr: 0x51080b00                A2,NA  A2,NA  NA    NA

reachable domains:
1 2 4 5 6 7 8 9 10 11 12 14 15 16 17 18
16 domains reachable
Ports used for EFP/BF/DIA flood:
4 42

Command Statistics:
command    high(ms)  low(ms)   ave(ms)   total      dropped
=========================================================
fc_write   151       1         0         655        N/A
P Timer    0         0         0         0          N/A
BF Timer   42        31        35        9          N/A
<output truncated>
switch:admin>
```

See Also `supportshow`

fandisable

Disable a fan unit.

Syntax `fandisable` *unit*

Availability Admin

Description Use this command to disable a non-faulty fan unit by setting the RPM speed to 0.

Operand This command has the following operand:

unit	Specify the fan's unit number. View the fan unit numbers using the **fanshow** command. This operand is required.

Example To disable a fan unit:

```
switch:admin> fandisable 1

Fan unit 1 has been disabled
switch:admin>
```

See Also
`fanshow`
`fanenable`

fanenable

Enable a fan unit.

Syntax `fanenable` *unit*

Availability Admin

Description Use this command to set the fan unit back to the default RPM speed only if the fan unit has been previously disabled using the `fandisable` command.

Operand This command has the following operand:

unit	Specify the fan's unit number. View the fan unit numbers using the `fanshow` command. This operand is required.

Example **To enable a fan that has been disabled:**

```
switch:admin> fanenable 1

Fan unit 1 has been enabled
switch:admin> fanshow

Fan #1 is OK, speed is 2237 RPM
Fan #2 is OK, speed is 2500 RPM
Fan #3 is OK, speed is 2445 RPM
```

See Also

```
fanshow
fandisable
```

fanshow

Display fan status.

Syntax `fanshow`

Availability All users

Description Use this command to display the current status of the switch fans. The format of the display varies according to the switch model and number of fans. Some switch models show fan speed measured in RPM (revolutions per minute).

Fan status is shown as:

OK	Fan is functioning correctly.
absent	Fan is not present.
below minimum	Fan is present but rotating too slowly or stopped.
unknown	Unknown fan unit installed.
faulty	Fan has exceeded hardware tolerance.

The output from this command varies depending on switch type and number of fans present.

Operand None

Example **To display the status and RPMs for the fans:**

```
switch:admin> fanshow
Fan #1 is OK, speed is 2721 RPM
```

```
Fan #2 is OK, speed is 2721 RPM
Fan #3 is OK, speed is 2657 RPM
switch:admin>
```

See Also

```
fandisable
fanenable
psshow
tempshow
chassisshow
```

fastboot

Reboot the switch, bypassing POST.

Syntax `fastboot`

Availability Admin

Description Use this command to reboot the switch, bypassing Power On Self Test (POST). The reboot takes effect immediately as the switch resets and executes normal power-on booting sequence. However, POST is skipped. This reduces boot time significantly.

If POST has been disabled using the `diagdisablepost` command, then `fastboot` is the same as reboot. However, `fastboot` skips the POST on the current reboot, while `diagdisablepost` skips POST on all future reboots until cancelled by `diagenablepost`.

Because `fastboot` reboots the CP a WARNING message and a confirmation is displayed. The command only takes place if the user responds positively.

For the ED-12000B, the `fastboot` command will reboot both logical switches and both CPs.

Operands None

Example Perform a reboot with no POST:

```
switch:admin>fastboot

Warning: This command is being run on a control processor (CP)
based system and will cause the active CP to reboot. 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
```

See Also
- diagdisablepost
- diagenablepost
- switchreboot
- reboot

fazoneadd

Add a member to a Fabric Assist zone.

Syntax `fazoneadd "fazoneName","member; member"`

Availability Admin

Description Use this command to add one or more members to an existing Fabric Assist zone.

This command does not change the defined configuration (which you can view using the `cfgshow` command) until the `cfgsave` command is issued. For the change to become effective, an appropriate Fabric Assist zone configuration must be enabled using the `cfgenable` command. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands This command has the following operands:

fazoneName	Specify the name for the Fabric Assist zone in quotation marks. This operand is required.

member — Specify a list of Fabric Assist Zone members. The list must be enclosed in quotation marks, and each member must be separated by a semi-colon. A member can be specified by one or more of the following methods:

- Enter a fabric domain and area number pair. View the area numbers for ports using the `switchshow` command.
- WWNs;
- Fabric Assist zone alias names;
- Exactly one Fabric Assist host member.

This operand is required.

Example **To add aliases for some disk arrays to "Blue_fazone":**

```
switch:admin> fazoneadd "Blue_fazone", "array3; array4; array5"
```

To add a Fabric Assist host member to "Blue_fazone":

```
switch:admin> fazoneadd "Blue_fazone", "H{5,6}"
```

See Also

```
fazonecreate
fazonedelete
fazoneremove
fazoneshow
```

fazonecreate

Create a Fabric Assist zone.

Syntax `fazonecreate "fazoneName","member; member"`

Availability Admin

Description Use this command to create a new Fabric Assist zone. You must specify a name and member list for a Fabric Assist zone. The FA zone name must be unique from any previously used Fabric Assist zone object. The member list must be enclosed in quotation marks and each member must be separated by a semicolon.

A Fabric Assist zone name is a C language-style name. It must begin with a letter and be followed by any number of letters, digits and underscore characters. Names are case sensitive, for example `Zone_1`

and fazone_1 are different Fabric Assist zones. White space is ignored.

The Fabric Assist zone member list must have at least one FA host and one target member. Empty lists are not allowed.

When a Fabric Assist zone member is specified by physical fabric port number, then any and all devices connected to that port are in the Fabric Assist zone. If this port is an arbitrated loop, then all devices on the loop are in the Fabric Assist zone.

WWNs are specified as eight hex numbers separated by colons, for example 10:00:00:60:69:00:00:8a. Zoning has no knowledge of the fields within a WWN; the eight bytes are simply compared with the Node and Port Names presented by a device in a login frame (FLOGI or PLOGI).

When a Fabric Assist zone member is specified by Node Name, then all ports on that device are in the Fabric Assist zone. When a Fabric Assist zone member is specified by Port Name, only that single device port is in the Fabric Assist zone. Zone alias names have the same format as Fabric Assist zone names and are created with the **alicreate** command. The alias must resolve to a list of one or more physical fabric port numbers, WWNs, or a Fabric Assist host.

A Fabric Assist host member is defined by wrapping the physical fabric port or a physical device (a WWN) between H{ and }. For example, H{5,6} or H{10:00:00:60:69:00:00:8a} is a Fabric Assist host. The type of Fabric Assist zone members used to define a Fabric Assist zone may be mixed and matched. For example, a Fabric Assist zone defined with the following members: 2,12; 2,14; 10:00:00:60:69:00:00:8a would contain devices connected to switch 2, ports 12 and 14, and the device with a WWN of 10:00:00:60:69:00:00:8a (either Node Name or Port Name - whichever port in the fabric it is connected to.)

This command does not change the defined configuration (which you can view using the cfgshow command) until the cfgsave command is issued. For the change to become effective, an appropriate Fabric Assist zone configuration must be enabled using the cfgenable command. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the cfgsave command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands The following operands are required:

fazoneName Specify a name for the Fabric Assist zone. The name must be enclosed in quotation marks. This operand is required.

member Specify a member or list of members to add to a Fabric Assist zone. The list must be enclosed in quotation marks, and each member must be separated by a semi-colon. A member can be specified by one or more of the following methods:

- Enter a fabric domain and area number pair. View the area numbers for ports using the `switchshow` command.
- WWNs;
- Fabric Assist zone alias names;
- Exactly one Fabric Assist host member.

This operand is required.

Example **To create three Fabric Assist zones using a mixture of port numbers and Fabric Assist zone aliases:**

```
switch:admin> fazonecreate "fazone1", "H{1,0}; loop1"
switch:admin> fazonecreate "fazone2", "H{1,1}; array1; 1,2; array2"
switch:admin> fazonecreate "fazone3", "1,0; loop1; H{1,2}; array2"
```

See Also

```
fazoneadd
fazonedelete
fazoneremove
fazoneshow
```

fazonedelete

Delete a Fabric Assist mode zone.

Syntax `fazonedelete "fazonename"`

Availability Admin

Description Use this command to delete an existing Fabric Assist mode zone on a fabric.

This command does not change the defined configuration (which you can view using the `cfgshow` command) until the `cfgsave` command is issued. For the change to become effective, an appropriate Fabric Assist zone configuration must be enabled using the `cfgenable` command. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands The following operand is required:

fazonename	Specify the name of the zone to be deleted, in quotation marks.

Example **To delete a Fabric Assist zone:**

```
switch:admin> fazonedelete "Blue_fazone"
```

See Also `fazonecreate`

fazoneremove

Remove members from a Fabric Assist mode zone.

Syntax `fazoneremove "fazoneName", "member; member"`

Availability Admin

Description Use this command to remove one or more members from an existing Fabric Assist zone.

Each deleted member must be found by an exact string match. Order is important when removing multiple members of a Fabric Assist zone. For example, if a Fabric Assist zone contains `array2; array3; array4` then removing `array4; array3` fails, but removing `array3; array4` succeeds. If issuing this command results in all members being removed, the Fabric Assist zone is deleted.

This command does not change the defined configuration (which you can view using the `cfgshow` command) until the `cfgsave` command is issued. For the change to become effective, an appropriate Fabric Assist zone configuration must be enabled using the `cfgenable` command. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands The following operands are required:

fazoneName	Specify a name for the Fabric Assist zone in quotation marks. This operand is required.
member	Specify a member or list of members to remove from a Fabric Assist zone. The list must be enclosed in quotation marks, and each member must be separated by a semi-colon. A member can be specified by one or more of the following methods: • Enter a fabric domain and area number pair. View the area numbers for ports using the `switchshow` command. • WWNs; • Fabric Assist zone alias names; • Exactly one Fabric Assist host member.

This operand is required.

Example **To remove "array2" from "Blue_fazone":**

```
switch:admin> fazoneremove "Blue_fazone", "array2"
```

See Also

```
fazoneadd
fazonecreate
fazonedelete
fazoneshow
```

fazoneshow

Display fazone information.

Syntax `fazoneshow ["pattern"[, transflag]]`

Availability All users

Description Use this command to display fazone information. Specifying this command with no parameters or with the second parameter set to zero displays all fazone configuration information for both Defined and Effective configurations. Defined configuration information is shown from the transaction buffer. Refer to the `cfgshow` command for a description of this display.

If a parameter is specified, it is used as a pattern to match fazone names, and those that match in the Defined configuration are displayed.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

pattern Specify a value to search for the name of an fazone. This can be any POSIX style expression. Patterns can contain:

- Question mark ? that matches any single character
- Asterisk * that matches any string of characters
- Ranges which match any character within the range.
  For example, [0-9] or [a-f].

This operand is optional.

transflag Specify 0 to display the information from the current transaction, or specify 1 to display information from the original buffer. This operand must be preceded by a pattern.

Example **To display all fazones beginning with the letters A through C:**

```
switch:admin> fazoneshow "[A-C]*"
          fazone:  Blue_fazone
                   1,1; array1; 1,2; array2
```

See Also

```
fazoneadd
fazonecreate
fazonedelete
fazoneremove
```

fcpprobeshow

Display the fcp probe information.

Syntax `fcpprobeshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display the fcp probing information for a particular device which should be of type F/FL port. If the given port is not either of the above types, then the following is displayed:

```
port x is not an FL_Port or an F_Port
```

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the fcp probe information:**

```
switch:admin> fcpprobeshow 4/4

port 52 is L-Port and it is online.
nodes probed:           2
successful PLOGIs:      2
successful PRLIs:       2
successful INQUIRies:   2
successful LOGOs:       2
outstanding IUs:        0

list of devices(may include old devices on the loop):
0x2b4e2: IBM     DDYF-T09170R    F60N
0x2b4e4: IBM     DDYF-T09170R    F60N
switch:admin>
```

See Also

```
portloginshow
portshow
```

fcprlsshow

Display the fcp rls information.

Syntax `fcprlsshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display the fcp rls (read link state) information for a particular device which should be of type F/FL port.If the given port is not either of the above types, then the following is displayed:

```
port x is not an FL_Port or an F_Port
```

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number

5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the fcp rls information:**

```
switch:admin> fcprlsshow 9/1

       link fail   loss sync   loss sig   prtc err   bad word   crc err

switch:admin>
```

See Also
```
portloginshow
portshow
```

fdmicacheshow

Display abbreviated remote FDMI device information according to remote domain ID.

Syntax `fdmicacheshow`

Availability All users

Description Use this command to display FDMI cache information for remote domains only.

The state of each remote domain, identified by its domain ID, is shown to be either UNKNOWN, KNOWN, UNSUPPORTED, or ERROR.

The revision of FDMI supported is also shown followed by the identifiers of all the HBAs at the domain and the corresponding registered port list.

For HBAs, only the HBA identifiers and registered port lists are show. No detailed HBA attributes are displayed. For registered ports, only its port identifier and its corresponding HBA are shown. No detailed port attributes are displayed.

Operands None

Example To display the FDMI cache:

```
switch:admin> fdmicacheshow
Switch entry for domain 1
  state:    known
  version:  v410
  wwn:      10:00:00:60:69:80:4f:85

    No devices.
  Total count of devices on the switch is 0

switch:admin>
```

See Also `fdmishow`

fdmishow

Display detailed FDMI device information.

Syntax `fdmishow`

Availability All users

Description Use this command to display FDMI information for all HBAs and ports.

Detailed FDMI information is displayed for local HBAs and ports. This information includes the HBA with its corresponding ports, along with their respective attributes.

Only abbreviated FDMI information is shown for HBA and ports on remote switches.

Operands None.

Example To display FDMI information on a local switch:

```
switch:admin> fdmishow
Local HBA database contains:
  10:00:00:00:c9:25:9b:96
  Ports: 1
    10:00:00:00:c9:25:9b:96
      Port attributes:
       FC4 Types: 0x0000010000000001000000000000000000000000000000000000000000000000
   000000000
        Supported Speed: 0x00000001
        Port Speed: 0x00000001
        Frame Size: 0x00000800
  HBA attributes:
    Node Name: 20:00:00:00:c9:25:9b:96
    Manufacturer: Emulex Corporation
    Serial Number: 0000c9259b96
    Model: LP9000
    Model Description: Emulex LightPulse LP9000 1 Gigabit PCI Fibre Channel
   Adapter
    Hardware Version: 1002806D
    Driver Version: 5-5.00A6
    Firmware Version: 3.81A1
    OS Name and Version: Windows 2000
    Max CT Payload Length: 0x00ff0000

Local Port database contains:
  10:00:00:00:c9:25:9b:96

Remote HBA database contains:
  10:00:00:00:c9:26:0f:e4
  Ports: 1
    10:00:00:00:c9:26:0f:e4

Remote Port database contains:
  10:00:00:00:c9:26:0f:e4

switch:admin>
```

For managing a remote switch:

```
switch:admin> fdmishow
FDMI LOCAL_HBA hash contains no entry.

FDMI LOCAL_PORT hash contains no entry.

FDMI REMOTE_HBA hash contains:
  Id: 10:00:00:00:c9:25:9b:96

Port List: total 1 port(s)
  Id: 10:00:00:00:c9:25:9b:96
  Port attributes:

  <No attribute information for remote HBAs.>

FDMI REMOTE_PORT hash contains:
  Id: 10:00:00:00:c9:25:9b:96
```

See Also `fdmicacheshow`

filtertest

Frame Filter test.

Syntax `filtertest [-passcnt` *passcnt*`] [-txports` *list*`] [-scamoff` *offset*`] [-dcamoff` *offset*`] [-fdefoff` *offset*`]`

Availability Admin

Description Use this command to verify that the ASIC frame level filtering logic including every type of filter actions:

- FLTACT_LIST_A - action to handle the subgroup A based filtering
- FLTACT_LIST_B - action to handle the subgroup B based filtering
- FLTACT_FROZEN - action to handle the frame frozen process
- FLTACT_DISCARD - action to discard frame
- FLTACT_FORWARD - action to forward frame

This command can be run on every port, and send the frame in internal loop back mode. The filter test requires two different ports in same quadrant due to the fact that the filter logic sits in transmitter port can not work if frame is sent directory from the embedded port.

In this test, the filter definition covers the filtering conditions shown in Table 1-7:

Table 1-7 List of Filter Test Numbers, Definitions, and Action Types

Number	Filter Definition	Action Type
0	unconditional match	Forward
1	unconditional match	List A
2	unconditional match	List B
3	unconditional match	Frozen
4	unconditional match	Discard
5	SCAM no match and ALPA match	List A
6	SCAM&DCAM match and ALPA match	List A
7	Zone A match and ALPA match	List A
8	Zone B match and ALPA match	List B
9	Zone A&B match and ALPA match	List B
10	Zone A | B match and ALPA match	Frozen
11	Zone A | B match and ALPA match	Discard

Operands This command has the following operands:

`-passcnt` *`passcnt`* Specify the number of times to perform this test. The default value is 1.

`-txports` *`list`* Specify the user port number(s) to perform this test. All user ports are set in default.

`-scamoff` *`offset`* Specify the program location to write SCAM test data in SCAM memory. The default value is 0. The maximum offset number is set if the specified number is larger than limit.

`-dcamoff` *`offset`* Specify the program location to write DCAM test data in DCAM memory. The default value is 0. The maximum offset number is set if the specified number is larger than limit.

`-fdefoff offset` Specify the program location to write filter test definition data in filter definition memory. The default value is 0. The maximum offset number is set if the specified number is larger than limit.

Example **To run a frame filter test:**

```
switch:admin> filtertest -txports 3/1-3/3

Running filtertest ..............
Test Complete: filtertest Pass 1 of 1
Duration 0 hr, 0 min & 2 sec (0:0:2:679).
 passed.
```

Errors When it detects failure(s), the subtest may report one or more of the following error messages:

```
DIAG-ACTTEST
DIAG-FLTINIT
DIAG-FLTRCV
DIAG-FLTXMIT
DIAG-NUMTEST
```

See Also `itemlist`

firmwarecommit

Commit switch firmware update.

Syntax `firmwarecommit`

Availability Admin

Description Use this command to commit a firmware download to a CP. This command copies an updated firmware image to both partitions and commits both partitions of a CP to an updated version of the firmware. This must be done after each `firmwaredownload`, and after the switch has been rebooted and a sanity check is performed to make sure the new image is fine.

For switches which have flash memory set into two equal partitions, the primary partition is the where the system boots from, the secondary partition is where a copy of the firmware is stored, in case the primary partition is damaged.

To maintain the integrity of the firmware image in the flash memory, the `firmwaredownload` command updates the secondary partition

only. When `firmwaredownload` completes successfully and the CP is rebooted, the system switches the primary partition (with the old firmware) to the secondary, and the secondary partition (with the new firmware) to the primary.

The default behavior of the `firmwaredownload` command automatically runs the `firmwarecommit` command after the reboot. For the cautious, the `firmwaredownload` command has an option to disable auto-commit of the new firmware. If you decide to disable the auto-commit option when running `firmwaredownload`, then, after the CP is rebooted, you must execute one of two commands:

- run the `firmwarecommit` command to copy the primary partition (with new firmware) to the secondary, and commit the new firmware to both partitions of the CP.
- or, run the `firmwarerestore` command to copy the secondary partition (with the old firmware) to the primary, and back out of the new firmware download. The `firmwarerestore` command can only be run if auto-commit was disabled during the firmwaredownload.

Operands None

Example **To commit a new version of the firmware:**

```
switch:admin> firmwarecommit
Doing firmwarecommit now.
Please wait ...
.....
.....
.....
.....
.....
......
Replicating kernel image
.............
FirmwareCommit completes successfully.
switch:admin>
```

See Also

```
firmwaredownload
firmwarerestore
```

firmwaredownload

Download switch firmware from a remote host or from a local directory.

Syntax `firmwaredownload [ [-sbn] host,user,pfile,passwd]`

Availability Admin

Description Use this command to download switch firmware from a FTP server or from a local (NFS) directory to the switch's non-volatile storage area.

The new firmware is in the form of RPM packages with names defined in a pfile. pfile is a binary file which contains specific firmware information (time stamp, platform code, version, etc.) and the names of packages of the firmware to be downloaded. These packages are made available periodically to add features or to remedy defects. Contact customer support to obtain information about available firmware versions.

In the ED-12000B, this command by default downloads firmware image to both CPs in a rollover mode to prevent disruption to application services. This operation depends on HA support. If HA is not available, a user will still be able to upgrade the CPs one at a time using `-s` option.

TheDS-32B2 and each CP of the ED-12000B have two partitions of non-volatile storage areas, a primary and a secondary, to store two firmware images. `Firmwaredownload` will always load the new image into the secondary partition and will swap the secondary partition to be the primary. It will then reboot the CP and activate the new image. Finally, it will perform `firmwarecommit` automatically to copy the new image to the other partition unless "-s" is used.

The command supports both non-interactive and interactive modes. If it is invoked without any command line parameters, or if there is any syntax error in the parameters, the command will go into the interactive mode in which the user is prompted for input.

Refer to the *Fabric OS Procedures Guide* **Firmware Download** chapter for limitations when changing Fabric OS versions. When installing Fabric OS v4.1, the procedure may vary depending on which version of the Fabric OS you are migrating from.

Operands This command has the following operands:

`-s`	Specify this operand to enable Single CP Mode. In the ED-12000B, this mode enables a user to upgrade a single CP and to select full-install, auto-reboot, and auto-commit. In the DS-32B2, this mode enables a user to select full-install, auto- reboot, and auto-commit.
`-b`	Specify this operand to activate auto-reboot mode. After downloading firmware the system must be rebooted. If this operand is not specified, the user must issue the `reboot` command manually in order to activate the downloaded image. If Auto-reboot mode is enabled, the switch reboots automatically after the `firmwaredownload` command has been run.
`-n`	Specify this operand to de-activate auto-commit mode. By default, after running this command and after `reboot`, the switch will perform a `firmwarecommit` command automatically. When this mode is disabled, the user needs to issue the `firmwarecommit` command manually to replicate the downloaded image to both partitions of a CP.
`host`	Specify a host server name or IP address; for example, `citadel` or `123.123.123.123`. The pfile is downloaded from this host system. If this operand is not used, the pfile is considered to be accessible through a local directory. This operand is required.
`user`	Specify a user name for FTP server access; for example, `jdoe`. This user name is used to gain access to the host. This operand is required.
`pfile`	Specify a fully qualified path and file name; for example, `/pub/dist/system.plist`. Absolute path names may be specified using forward slash (/). Relative path names create the file in the user's home directory on UNIX hosts, and in the directory where the FTP server is running on Windows hosts. This operand is required.
`passwd`	Specify a password. This operand is required, but may be NULL.

If no operand is specified the operation becomes interactive and you are prompted for input.

Example To download the firmware to a HA switch:

```
switch:admin> firmwareDownload
   192.168.166.30,johndoe,/pub/dist/release.plist,12345
You can run firmwareDownloadStatus from a telnet session to
get the status of this command.

This command will cause the active CP to reset. This will
cause disruption to devices attached to both switch 0 and
switch 1 momentarily and will require that existing telnet
sessions be restarted.

Do you want to continue [Y]: y

FirmwareDownload has started in Standby CP. It may take up to 10 minutes.

And you will the following on Standby CP:

Start to install packages......
dir                  ###################################################
terminfo             ###################################################
termcap              ###################################################
glibc                ###################################################
sin                  ###################################################
Write kernel image into flash.
Verification SUCCEEDED
Firmwaredownload completes successfully.
```

Errors The following can cause the download to fail:

- Host is not known to the switch
- Host cannot be reached by the switch
- User does not have permission on host
- The pfile does not exist on host
- The pfile is not in the right format
- Package specified in the pfile doesn't exist
- The FTP server is not running on host
- Running firmwaredownload during POST
- A loss of power to the switch

See Also

```
switchreboot
reboot
version
```

firmwaredownloadstatus

Display the status of a firmware download.

Syntax `firmwaredownloadstatus`

Availability Admin

Description Use this command to display an event log that records the progress and status of the current `firmwaredownload` command. The event log is created by the current `firmwaredownload` command and is kept until another `firmwaredownload` command is issued. There is a timestamp associated with each event.

In a ED-12000B, when `firmwaredownloadstatus` is run, the event logs in the two CPs are synchronized. The command can be run from either CP.

Operands None

Example To display the status of a firmware download:

```
switch:admin> firmwaredownloadstatus
[1]: Tue Jan 18 13:21:25 2005
cp1: FirmwareDownload has started on Standby CP. It may take up to 10
   minutes.

[1]: Tue Jan 18 13:21:35 2005
cp1: FirmwareDownload has completed successfully on Standby CP.

[2]: Tue Jan 18 13:21:37 2005
cp1: Standby CP reboots.

[3]: Tue Jan 18 13:24:44 2005
cp1: Standby CP boots up.

[4]: Tue Jan 18 13:24:45 2005
cp1: Standby CP booted up with new firmware.

<output truncated>

[9]: Tue Jan 18 13:33:54 2005
cp0: Standby CP booted up with new firmware.

[10]: Tue Jan 18 13:33:56 2005
cp0: Firmwarecommit has started on both Active and Standby CPs.

[11]: Tue Jan 18 13:38:29 2005
cp0: FirmwareCommit has completed successfully on Active CP.

[12]: Tue Jan 18 13:38:30 2005
cp0: FirmwareDownload has completed successfully.
```

See Also `firmwaredownload`
`firmwarecommit`
`firmwarerestore`
`firmwareshow`

firmwarerestore

Restore old active firmware image.

Syntax `firmwarerestore`

Availability Admin

Description Use this command to restore the old active firmware image. This command can only be run if auto-commit was disabled during the `firmwaredownload`.

After a `firmwaredownload` and a `reboot` (with auto-commit disabled), the downloaded firmware will become active. If you then do not want to commit the firmware, and instead want to restore the old firmware, run `firmwarerestore`. After running `firmwarerestore`, you can run `firmwaredownload` again.

This command will reboot the system and make the old firmware active. After reboot, both primary and secondary partitions are restored to the old firmware.

This command will only take action if the system is booted after a `firmwaredownload`. Otherwise, it will return with an error code.

Operands None

Example To restore old active firmware image:

```
switch:admin> firmwarerestore
Restore old image to be active ...
Restore both primary and secondary image after reboot.
The system is going down for reboot NOW !!
Broadcast message from root (ttyS0) Fri Oct 26 23:48:54 2001...


Doing firmwarecommit now.
Please wait ...
```

See Also `firmwaredownload`
`firmwarecommit`

firmwareshow

Display the Fabric OS versions on both partitions of the local and remote CPs.

Syntax `firmwareshow`

Availability Admin

Description Use this command to display the Fabric OS versions on primary and secondary partitions on the local CP and on the remote CP. This command identifies the status for each CP as Active or Standby, and will also identify the slot number for each CP.

If there is only one CP available, the command displays the Fabric OS versions for the primary and secondary partitions on that CP.

Operands None

Example **To display the firmware version of aDS-3252:**

```
switch:admin> firmwareshow
Primary partition:      v4.1.0
Secondary Partition:    v4.1.0
switch:admin>
```

To display the firmware version of a ED-12000B:

```
switch:admin> firmwareshow
Local CP (Slot 6, CP1): Active
        Primary partition:      v4.1.0
        Secondary Partition:    v4.1.0
Remote CP (Slot 5, CP0): Standby
        Primary partition:      v4.1.0
        Secondary Partition:    v4.1.0

Note: If Local CP and Remote CP have different versions
of firmware, please retry firmwaredownload command.
switch:admin>
```

See Also `firmwaredownloadstatus`

fporttest

Functional test of F->N, N->F point to point path.

Syntax

```
fporttest [-nframes count] [-ports itemlist] [-seed
payload_pattern] [-width pattern_width]
[-size pattern_size]
```

Availability

Admin

Description

Use this command to verify the functional operation of the switch by sending els ECHO frames from switch F_Port's transmitter, and receive els ECHO ACC back from N_Port device into F_Port's receiver. This exercises all the switch components from the main board to the SFP, to the fiber cable, to the SFPs (of the N_Port devices and the switch F_Port), and back to the main board.

The cables and SFPs connected should be of the same technology; that is, a short wavelength SFP (switch) port is connected to another short wavelength SFP (device) port using a short wavelength cable; and a long wavelength port is connected to a long wavelength port; and a copper port is connected to a copper port.

Only one frame is transmitted and received at any one time. The port LEDs flicker green rapidly while the test is running.

The test method is as follows:

1. Determine which ports are F_Port
2. Create a ELS_ECHO frame with payload size, data pattern build in, or payload size, data pattern.
3. Transmit frame F via F_Port, with D_ID to the N_Port device.
4. Wait for N_Port device to response ECHO ACC.
5. Compare ECHO data transmitted is equal to the ECHO data received.
6. Repeat steps 3 through 5 for all ports present until:
   a. the number of frames requested is reached,
   b. all ports are marked bad.

You can specify a payload pattern to be used when executing this test. If the pattern is not user specified, then at every 30 pass, a different data type from a palette of seven is used to generate different data

pattern to create the frame. The data pattern will be generated based on each data type. Some data types may generate different data pattern on every pass, and other data type may not change the data pattern in every pass. These seven data types will be repeated every 210 pass. The data palette is as follows:

```
1) CSPAT:       0x7e, 0x7e, 0x7e, 0x7e, ...
2) BYTE_LFSR:   0x69, 0x01, 0x02, 0x05, ...
3) CHALF_SQ:    0x4a, 0x4a, 0x4a, 0x4a, ...
4) QUAD_NOT:    0x00, 0xff, 0x00, 0xff, ...
5) CQTR_SQ:     0x78, 0x78, 0x78, 0x78, ...
6) CRPAT:       0xbc, 0xbc, 0x23, 0x47, ...
7) RANDOM:      0x25, 0x7f, 0x6e, 0x9a, ...
```

Operands

This command has the following operands:

`-nframes` *count*
: Specify the number of times (or number of frames per port) to execute this test. If omitted, the default value used is 10. This operand is optional.

`-ports` *itemlist*
: Specify the ports to run to test on. If omitted, the test will be executed on all online F_ports in the specified slot. This operand is optional.

`-seed` *payload_pattern*
: Specify the pattern of the test packets payload. When payload_pattern is set to 0, all seven different data types will be used. This operand is optional.

`-width` *pattern_width*
: Specify the width of the pattern which user specified. When *payload_pattern* is set to 0x00, *pattern_width* will be ignored. Valid values are:

  1 = byte
  2 = word
  4 = quad

  This operand is optional.

`-size` *pattern_size*
: Specify the number of words of the test packets payload. If omitted, the default value is 512. This operand is optional.

Example **To run an fporttest on a switch:**

```
switch:admin> fporttest -ports 1/0-1/15
Running fPortTest .......
Test Complete: "fporttest" Pass 10 of 10
Duration 0 hr, 0 min & 1 sec (0:0:0:127).
passed.
switch:admin>
```

Errors Below are possible error messages if failures are detected:

```
DATA
INIT
PORT_DIED
EPI1_STATUS_ERR
ERR_STAT
ERR_STATS
ERR_STATS_2LONG
ERR_STATS_BADEOF
ERR_STATS_BADOS
ERR_STATS_C3DISC
ERR_STATS_CRC
ERR_STATS_ENCIN
ERR_STATS_ENCOUT
ERR_STATS_TRUNC
ERR_STAT_2LONG
ERR_STAT_BADEOF
ERR_STAT_BADOS
ERR_STAT_C3DISC
ERR_STAT_CRC
ERR_STAT_ENCIN
ERR_STAT_ENCOUT
ERR_STAT_TRUNC
FDET_PERR
FINISH_MSG_ERR
FTPRT_STATUS_ERR
LESSN_STATUS_ERR
MBUF_STATE_ERR
MBUF_STATUS_ERR
NO_SEGMENT
PORT_ABSENT
PORT_ENABLE
PORT_M2M
PORT_STOPPED
PORT_WRONG
RXQ_FRAME_ERR
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FRX
STATS_FTX
TIMEOUT
```

XMIT

See Also

itemlist
crossporttest
loopporttest
spinfab
porttest

frureplace

Interactive interface to replace a Field Replaceable Unit (FRU).

Syntax `frureplace` *FRUtype*

Availability Admin

Description Use this command to guide you in replacing a ED-12000B FRU. The command automatically performs the necessary backup and restore steps to accommodate the replacement. This command must be entered through the active CP card.

Operands This command has the following operands:

FRUtype	Specify the type of hardware component being replaced. For Fabric OS v4.1, `WWN` is the only supported operand, and specifies the replacement of the WWN card.

Example To replace the world wide name card:

```
switch:admin>frureplace wwn
This is the WWN card hot swap interface.
Continuing from this point will require
the whole process to be completed.
If this process is not complete due to a
power cycle, or CP failover, please follow
the recovery procedure in
Core Switch  WWN Card Removal and
Replacement document.
Do you wish to continue [y/n]? Y

Backing up WWN card data, please
wait about 25 seconds for further
instruction.

Ready to restore WWN card data, please make
sure you have a replacement FRU now.

If this session lost due to user aborted,
please reinitiate the invoking command and
follow the instructions to complete the
operation.

Please enter the word `continue' when done: continue
Restoring the replacement FRU now,
please wait about 20 seconds to complete
Verifying the replacement FRU now...
WWN card hot swap is now complete.
FRU replacement completed successfully!
```

fspfshow

Display FSPF protocol information.

Syntax `fspfshow`

Availability All users

Description Use this command to display the Fibre Channel Shortest Path First (FSPF) protocol information, and internal data structures. FSPF is implemented by a single task, called tFspf.

The display shows the fields shown in Table 1-8:

Table 1-8 fspfshow Display Fields

Field	Description
version	Version of FSPF protocol.
domainID	Domain number of local switch.
switchOnline	State of the local switch.
domainValid	Domain of the local switch is currently confirmed.
isl_ports	Bit map of all E_Ports.
trunk_ports	Bit map of all the trunk ports.
f_ports	Bit map of all the Fx_Ports.
seg_ports	Bit map of all the segmented ports.
active_ports	Bit map of all the ONLINE ports.
minLSArrival	FSPF constant.
minLSInterval	FSPF constant.
LSoriginCount	Internal variable.
startTime	Start time of tFspf task (milliseconds from boot).
fspfQ	FSPF input message queue.
fabP	Pointer to fabric data structure.
agingTID	Aging timer ID.
agingTo	Aging time out value, in milliseconds.
lsrDlyTID	Link State Record delay timer ID.
lsrDelayTo	Link State Record delay time out value, in milliseconds.
lsrDelayCount	Counter of delayed Link State Records.
ddb_sem	FSPF semaphore ID.
event_sch	FSPF scheduled events bit map.
lsrRefreshCnt	Internal variable.

Operands None

Examples **To display FSPF protocol information:**

```
switch:admin> fspfshow

version          = 2
domainID         = 131
switchOnline     = TRUE
domainValid      = TRUE
isl_ports[0]     = 0x00000060
trunk_ports[0]   = 0x00000090
f_ports[0]       = 0x7fffff0f
seg_ports[0]     = 0x00000000
active_ports[0]  = 0x7fffffff
minLSArrival     = 3
minLSInterval    = 5
LSoriginCount    = 0
startTime        = 32140
fspfQ            = 0x1006a638
fabP             = 0x1006a628
agingTID         = 0x1007f500
agingTo          = 10000
lsrDlyTID        = 0x1007f558
lsrDelayTo       = 5000
lsrDelayCount    = 508
ddb_sem          = 0x1006a700

fabP:
event_sch        = 0x0
switch:admin>
```

See Also

```
bcastshow
mcastshow
topologyshow
urouteshow
```

fwalarmsfilterset

Enable or disable alarms for Fabric Watch.

Syntax `fwalarmsfilterset [mode]`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to configure alarm filtering for Fabric Watch. By turning off the alarms, all non-environment class alarms are suppressed. By turning on the alarms, all class alarms are generated.

Operands This command has the following operand:

mode	Specify 1 to enable the alarms, 0 to disable the alarms. If no operand is specified, the default value is 0 (alarms are deactivated). This operand is optional.

Example To enable alarms in Fabric Watch:

```
switch:admin> fwalarmsfilterset
FW: Alarms are disabled
switch:admin> fwalarmsfilterset 1
FW: Alarms are enabled
switch:admin>
```

See Also `fwalarmsfiltershow`

fwalarmsfiltershow

Display alarm filtering for Fabric Watch.

Syntax `fwalarmsfiltershow`

Availability All users

This command requires a Fabric Watch License.

Description Use this command to display whether alarm filtering is enabled or disabled.

Operands None

Example **To display the status of alarm filtering in Fabric Watch:**

```
switch:admin> fwalarmsfiltershow
fw: alarms are enabled
switch:admin> fwalarmsfiltershow
FW: Alarms are disabled
```

See Also `fwalarmsfilterset`

fwclassinit

Initialize all classes under Fabric Watch.

Syntax `fwclassinit`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to initialize all classes under Fabric Watch. The command should only be used after installing Fabric Watch license to start licensed Fabric Watch classes.

Operands None

Example **To initialize all classes under Fabric Watch:**

```
switch:admin> fwclassinit
fwClassInit: Fabric Watch is updating...
fwClassInit: Fabric Watch has been updated.
```

```
switch:admin>
```

See Also

```
fwconfigreload
fwconfigure
fwshow
```

fwconfigreload

Reload the Fabric Watch configuration.

Syntax

```
fwconfigreload
```

Availability

Admin

This command requires a Fabric Watch License.

Description

Use this command to reload the Fabric Watch configuration. This command should only be used after downloading a new Fabric Watch configuration file from a host.

Operands

None

Example

To reload the saved Fabric Watch configuration:

```
switch:admin> fwconfigreload
fwConfigReload: Fabric Watch configuration reloaded.
switch:admin>
```

See Also

```
configupload
configdownload
fwclassinit
fwconfigure
fwshow
```

fwconfigure

Display and modify the Fabric Watch configuration and status.

Syntax `fwconfigure`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to display and modify threshold information for the Fabric Watch configuration. Switch elements monitored by Fabric Watch are divided into classes, which are further divided into areas. In addition, each area can include multiple thresholds.

The Fabric Watch classes and areas are provided in Table 1-9.

Table 1-9 fwConfigure Fabric Watch Classes and Areas

Class	Area
1: Environmental class	1 : Temperature 2 : Fan 3 : Power Supply
2: SFP class	1 : Temperature 2 : RXP 3 : TXP 4 : Current 5 : Voltage
3: Port class	1 : Link loss 2 : Sync loss 3 : Signal loss 4 : Protocol error 5 : Invalid words 6 : Invalid CRCS 7 : RXPerformance 8 : TXPerformance 9 : State Changes

Table 1-9 fwConfigure Fabric Watch Classes and Areas (*continued*)

Class	Area
4: Fabric class	1 : E-Port downs 2 : Fabric reconfigure 3 : Domain ID changes 4 : Segmentation changes 5 : Zone changes 6 : Fabric<->QL 7 : Fabric logins 8 : SFP state changes
5: E_Port class	1 : Link loss 2 : Sync loss 3 : Signal loss 4 : Protocol error 5 : Invalid words 6 : Invalid CRCS 7 : RXPerformance 8 : TXPerformance 9 : State Changes
6: F/FL Port (Optical) class	1 : Link loss 2 : Sync loss 3 : Signal loss 4 : Protocol error 5 : Invalid words 6 : Invalid CRCS 7 : RXPerformance 8 : TXPerformance 9 : State Changes
7: Alpa Performance Monitor class	1 : Invalid CRCS
8: EE Performance Monitor class	1 : Invalid CRCS 2 : RXPerformance 3 : TXPerformance

Table 1-9 fwConfigure Fabric Watch Classes and Areas (*continued*)

Class	Area
9: Filter Performance Monitor class	1 : Customer Define
10: Security class	1 : Telnet Violations 2 : HTTP Violations 3 : API Violations 4 : RSNMP Violations 5 : WSNMP Violations 6 : SES Violations 7 : MS Violations 8 : Serial Violations 9 : Front Panel Violations 10 : SCC Violations 11 : DCC Violations 12 : Login Violations 13 : Invalid Timestamps 14 : Invalid Signatures 15 : Invalid Certificates 16 : SLAP Failures 17 : SLAP Bad Packets 18 : TS Out of Sync 19 : No-FCS 20 : Incompatible Security DB 21 : Illegal Command
11: Switch Availability Monitor class	1 : Total Down time 2 : Total Up time 3 : Duration of Occurrences 4 : Fequency of Occurrences

Operands None

Example To display the Fabric Watch status for Temperature under the Environmental class:

```
switch:admin> fwconfigure

1  : Environment class
2  : SFP class
3  : Port class
4  : Fabric class
5  : E-Port class
6  : F/FL Port (Optical) class
7  : Alpa Performance Monitor class
8  : EE Performance Monitor class
9  : Filter Performance Monitor class
10 : Security class
11 : Quit
Select a class => : (1..11) [11] 1

1 : Temperature
2 : Fan
3 : Power Supply
4 : return to previous page
Select an area => : (1..4) [4] 1

Index ThresholdName                          Status       CurVal
          LastEvent                  LasteventTime      LastVal       LastState
=============================================================================
   =====
    1     envTemp001                          enabled        40 C
           inBetween     Wed Oct  9 15:34:24 2002         36 C      Normal
    2     envTemp002                          enabled        42 C
           inBetween     Wed Oct  9 15:34:24 2002         37 C      Normal
    3     envTemp003                          enabled        27 C
           inBetween     Wed Oct  9 15:34:24 2002         26 C      Normal
    4     envTemp004                          enabled        40 C
           inBetween     Wed Oct  9 15:34:24 2002         36 C      Normal
    5     envTemp005                          enabled        42 C
           inBetween     Wed Oct  9 15:34:24 2002         37 C      Normal

1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
Select choice => : (1..5) [5]
```

See Also fwclassinit
fwconfigreload
fwshow

fwfrucfg

Display or modify FRU state alert configuration.

Syntax `fwfrucfg`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to configure FRU states and actions. Based on these configuration settings Fabric Watch generates action when FRU state changes. To configure email alerts use `fwmailcfg`.

Operands None

Example To change FRU state alert configuration:

```
switch:admin> fwfrucfg

1   : Slot
2   : Power Supply
3   : Fan
4   : WWN
5   : Configure All
6   : Set All to Default
7   : Quit

Select an item  => : (1..7) [7] 2

                                        Alarm
 Id             Label     Status       State     Level     Freq
==========================================================
   1    Power Supply #1   enabled         1         0         1
   2    Power Supply #2   enabled         1         0         1

1 : change fru alarm state      5 : change fru status
2 : change fru alarm level      6 : apply fru configuration
3 : change alarm frequency      7 : cancel fru configuration changes
4 : change fru timebase         8 : return to previous page
Select choice => : (1..8) [8] 1
Enter Id Number : (1..2) [2]

Absent-1, Inserted-2, Ready-4
Up-8, On-16, Off-32, Faulty-64
Enter fru alarm state  => : (0..127) [1] 32

                                        Alarm
 Id             Label     Status       State     Level     Freq
==========================================================
   1    Power Supply #1   enabled         1         0         1
   2    Power Supply #2   enabled        32         0         1

1 : change fru alarm state      5 : change fru status
2 : change fru alarm level      6 : apply fru configuration
3 : change alarm frequency      7 : cancel fru configuration changes
4 : change fru timebase         8 : return to previous page
Select choice => : (1..8) [8] 8
```

See Also fwmailcfg
fwconfigure

fwhelp

Display Fabric Watch command information.

Syntax `fwhelp`

Availability All users

Description Use this command to display commands used to configure Fabric Watch.

Operands None

Example **To display a summary of Fabric Watch commands:**

```
switch:admin> fwhelp

fwAlarmsFilterSet       Configure alarms filtering for Fabric Watch
fwAlarmsFilterShow      Show alarms filtering for Fabric Watch
fwClassInit             Initialize all Fabric Watch classes
fwConfigure             Configure Fabric Watch
fwConfigReload          Reload Fabric Watch configuration
fwSetToCustom           Set boundary & alarm level to custom
fwSetToDefault          Set boundary & alarm level to default
fwShow                  Show thresholds monitored by Fabric Watch
fwMailCfg               Configure Fabric Watch Email Alert
fwFruCfg                Configure FRU state and notification
fwSamShow               Show availability monitor information
switchStatusPolicyShow  Show switch status policy parameters
switchStatusPolicySet   Set switch status policy parameters
switchStatusShow        Show overall switch status
tempShow                Show switch temp readings
sensorShow              Show sensor readings

switch:admin>
```

fwmailcfg

Configure email alerts in Fabric Watch.

Syntax `fwmailcfg`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to display or modify the configuration and status of the Fabric Watch Email Alert in the switch.

Switch elements monitored by Fabric Watch are divided into Classes and Email Alert are base on the classes. Each class can configure one mail address as the alert message's receiver.

For email alert to function correctly add CP0 and CP1 IP address and hostname to DNS and also set Domain Name and Name Server. The `ipaddrshow` and `dnsconfig` commands can be used to set and check this information.

Example To configure an email address recipient for the SFP class in Fabric Watch and then enable email alerts:

```
switch:admin> fwmailcfg

1  : Show Mail Configuration Information
2  : Disable Email Alert
3  : Enable Email Alert
4  : Send Test Mail
5  : Set Recipient Mail Address for Email Alert
6  : Quit
Select an item  => : (1..6) [6] 5

            Mail Config  Menu
    ------------------------------------
        1  : Environment class
        2  : SFP class
        3  : Port class
        4  : Fabric class
        5  : E-Port class
        6  : F/FL Port (Copper) class
        7  : F/FL Port (Optical) class
        8  : Alpa Performance Monitor class
        9  : End-to-End Performance Monitor class
        10 : Filter Performance Monitor class
        11 : Security class
        12 : Switch Availability Monitor class (SAM)
        13 : quit
Select an item  => : (1..13) [13] 2

---<continued on next page>---
```

```
Committing configuration...done.
Mail To: [jonDoe@bogus.com] fvales@bogus.com
Committing configuration...done.
Committing configuration...done.

Email Alert configuration succeeded!


1  : Show Mail Configuration Information
2  : Disable Email Alert
3  : Enable Email Alert
4  : Send Test Mail
5  : Set Recipient Mail Address for Email Alert
6  : Quit
Select an item  => : (1..6) [6] 3


            Mail Enable Menu
    ____________________________________
        1  : Environment class
        2  : SFP class
        3  : Port class
        4  : Fabric class
        5  : E-Port class
        6  : F/FL Port (Copper) class
        7  : F/FL Port (Optical) class
        8  : Alpa Performance Monitor class
        9  : End-to-End Performance Monitor class
        10 : Filter Performance Monitor class
        11 : Security class
        12 : Switch Availability Monitor class (SAM)
        13 : quit

Select an item  => : (1..13) [13] 2
Committing configuration...done.

Email Alert is enabled!

1  : Show Mail Configuration Information
2  : Disable Email Alert
3  : Enable Email Alert
4  : Send Test Mail
5  : Set Recipient Mail Address for Email Alert
6  : Quit
Select an item  => : (1..6) [6] 6
switch:admin>
```

See Also fwconfigure
fwclassinit

```
fwshow
fwconfigreload
```

fwsamshow

Display the switch availability monitor information.

Syntax `fwsamshow`

Availability All users

This command requires a Fabric Watch License.

Description Use this command to displays information about port availability. The information displayed includes: total uptime, total down time, number of faulty occurrences, and total percent of offtime for each port.

Operands None

Example The following example shows port summary information:

```
switch:admin> fwsamshow
                          Total      Total     Number Of    Total
Port#            Type     UpTime     DownTime  Occurences   OffTime
                          (Percent)  (Percent) (Times)      (Percent)
=========================================================================
  ==
 32              U_PORT     0          0          0          100
 33              U_PORT     0          0          0          100
 34              U_PORT     0          0          0          100
 35              U_PORT     0          0          0          100
 36              U_PORT     0          0          0          100
 37              U_PORT     0          0          0          100
 38              U_PORT     0          0          0          100
 39              U_PORT     0          0          0          100
 40              U_PORT     0          0          0          100
 41              U_PORT     0          0          0          100
 42              U_PORT     0          0          0          100
 43              U_PORT     0          0          0          100
 44              U_PORT     0          0          0          100
 45              E_PORT   100          0          0            0
 46              U_PORT     0          0          0          100
 47              U_PORT     0          0          0          100
 48              U_PORT     0          0          0          100
 49              U_PORT     0          0          0          100
 50              U_PORT     0          0          0          100
 51              E_PORT   100          0          0            0
 52              U_PORT     0          0          0          100
 53              U_PORT     0          0          0          100
 54              U_PORT     0          0          0          100
 55              U_PORT     0          0          0          100
 56              U_PORT     0          0          0          100
 57              U_PORT     0          0          0          100
 58              U_PORT     0          0          0          100
 59              E_PORT   100          0          0            0
 60              U_PORT     0          0          0          100
 61              U_PORT     0          0          0          100
 62              U_PORT     0          0          0          100
 63              U_PORT     0          0          0          100
switch:admin>
```

See Also switchshow

fwsettocustom

Set boundary and alarm levels to custom values.

Syntax `fwsettocustom`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to set boundary and alarm levels to custom for all classes and areas for Fabric Watch.

Operands None

Example **To set alarm levels to custom values:**

```
switch:admin> fwsettocustom
Committing configuration...done.
switch:admin>
```

See Also `fwsettodefault`

fwsettodefault

Set boundary and alarm levels to the default values.

Syntax `fwsettodefault`

Availability Admin

This command requires a Fabric Watch License.

Description Use this command to set boundary and alarm levels to default for all classes and areas for Fabric Watch.

Operands None

Example **To set alarm levels to default values:**

```
switch:admin> fwsettodefault
Committing configuration...done.
switch:admin>
```

See Also `fwsettocustom`

fwshow

Display the thresholds monitored by Fabric Watch.

Syntax `fwshow`

Availability All users

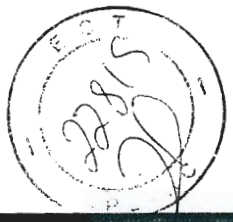
This command requires a Fabric Watch License.

Description Use this command to display the thresholds monitored by Fabric Watch.

This command can display a synopsis of thresholds for a particular class or more detailed information for an individual threshold.

The display of `fwshow` for root user could be different than admin user. The root user can see all inactive and active thresholds, but the admin user can only see active threshold.

Operands None



Example To display detailed Fabric Watch information on the envFan001 threshold:

```
switch:admin> fwshow

1  : Show class thresholds
2  : Detail threshold information
3  : Quit
Select an item  => : (1..3) [3] 2
Enter Threshold Name : [] envFan001

Env Fan 1:

   Monitored for:       28676 ( 7:57)
    Last checked:    23:32:14 on 10/09/2002

      Lower bound:        2600 RPM
      Upper bound:        7000 RPM
      Buffer Size:           3

   Value history:         3375 RPM

     Raw history:         3375 RPM
                          3409 RPM <output truncated>
                          3409 RPM

           Flags: 0x       40 TRIGGERED

    Counter:
      Access via: Function call
         Address: 0x1001b650
        Argument: 0x00000001

        Previous: 0x00000d2f (3375)
         Current: 0x00000d2f (3375)

         Events:
           Style: Triggered
             Event 0 occurred 1 time, last at 15:34:18 on 10/09/2002
             Event 1 occurred 268 times, last at 23:32:14 on 10/09 2002
           * Event 5 occurred 1 time, last at 15:34:24 on 10/09/2002

       Callbacks:
          2 callbacks are registered for event 3:
            0: 0x1001ad60  0x00000000
            1: 0x1001af30  0x00000000
          2 callbacks are registered for event 4:
            0: 0x1001ad60  0x00000000
            1: 0x1001af30  0x00000000
          1 callback is registered for event 5:
            0: 0x1001ad60  0x00000000

1  : Show class thresholds
2  : Detail threshold information
3  : Quit
Select an item  => : (1..3) [3] 3
```

See Also fwclassinit
fwconfigreload
fwconfigure

h

Display shell history.

Syntax `h`

Availability All users

Description Use this command to view the shell history. The shell history mechanism is similar to the UNIX Korn shell history facility. It has a built-in line editor similar to UNIX vi that enables previously typed commands to be edited. The command `h` displays the 20 most recent commands typed into the shell; old commands fall off the top as new ones are entered.

To edit a command, press ESC to access edit mode, then use vi commands. The ESC key switches the shell to edit mode. The ENTER key gives the line to the shell from either editing or input mode.

Basic vi commands:

`k`	get the previous shell command
`j`	get the next command
`h`	move the cursor left
`l`	move the cursor right
`a`	append
`i`	insert
`x`	delete
`u`	undo

Operands None

Example **To display previous shell commands:**

```
switch:admin> h
1 version
2 switchshow
3 portdisable 2
4 portenable 2
5 switchshow
```

hadisable

Disable the High Availability feature in the switch

Syntax `hadisable`

Availability Admin

Description Use this command to disable the High Availability feature in the Switch. If the HA feature is already disabled, this command does nothing.

Operands None

Example **To disable the High Availability feature:**

```
switch:admin> hadisable
Disabling HA ...
Done.
```

See Also `haenable`

hadump

Display information about the status of the High Availability feature in the switch

Syntax `hadump`

Availability All users

Description Use this command to display information about the status of the High Availability feature in the Switch. This command displays the following information:

- Local CP state (slot number and CP id);
- Remote CP state (slot number and CP id);
- High Availability Enabled/Disabled
- Heartbeat Up/Down
- Health of Standby CP. The Health of the Standby CP can show one of the following values:

Healthy	The Standby CP is running and the background health diagnostic has not detected any errors.

Failed — The Standby CP is running, but the background health diagnostic has discovered a problem with the blade. The logs should be checked to determine the appropriate repair action. Fail-over will be disabled until the Standby CP can be repaired.

- HA Synchronization Status. The HA Synchronization Status field can show one of the following values:

  HA State Synchronized — The system is currently fully synchronized. If a fail-over were necessary at this time, the fail-over would be non-disruptive.

  HA State Not In Sync — The system is unable to synchronize the two CPs, due to the Standby CP being faulty or another system error. If a fail-over were to take place at this time, the Standby CP would be rebooted, and the fail-over will be disruptive.

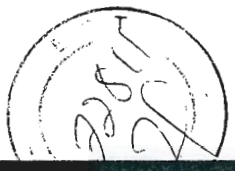
- IP and Fibre Channel addresses configured for the switch.
- Additional internal HA state information, subject to change.

Operands None

Example **To view information about the High Availability feature:**

```
switch:admin> hadump
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
SWITCH0
Ethernet IP Address: 10.64.118.104
Ethernet Subnetmask: 255.255.240.0
Fibre Channel IP Address: 0.0.0.0
Fibre Channel Subnetmask: 0.0.0.0

SWITCH1
Ethernet IP Address: 10.64.118.105
Ethernet Subnetmask: 255.255.240.0
Fibre Channel IP Address: 0.0.0.0
Fibre Channel Subnetmask: 0.0.0.0

--- <output truncated> ---
```

See Also `hafailover`
`hashow`



haenable

Enable the High Availability feature in the switch.

Syntax `haenable`

Availability Admin

Description Use this command to enable the High Availability feature in the Switch. If the HA feature is already enabled, this command does nothing.

Operands None

Example **To enable the High Availability feature in the switch:**

```
switch:admin> haenable
Enabling HA ...
Done.
switch:admin> haenable
HA is enabled
switch:admin>
```

See Also `hadisable`

hafailover

Forces the failover mechanism so that the Standby CP becomes the Active CP.

Syntax `hafailover`

Availability Admin

Description Use this command to force the failover mechanism to occur so that the Standby CP becomes the Active CP. Because `hafailover` results in CP reboot, a warning message and a confirmation is displayed. If the user answers positively, then the failover takes place.

On a ED-12000B, when HA synchronization is enabled and the CPs are in sync, if a failover is initiated, the port traffic light will not flash during the failover, even while traffic is continuing to flow.

Operands None

Example To force the failover of the active CP to the standby CP in the switch:

```
switch:admin> hafailover
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized

Warning: This command is being run on a control processor(CP)
based system. If the above status does not indicate HA State
synchronized then this operation 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 on the logical switch you intend to reboot.

Are you sure you want to reboot the active CP [y/n]? Y
```

See Also
- hadisable
- haenable
- hashow

hashow

Display control processor (CP) status.

Syntax hashow

Availability All users

Description Use this command to display the control processor status, which includes:

- Local CP state (slot number and CP id)
- Remote CP state (slot number and CP id)
- High Availability Enabled/Disabled
- Heartbeat Up/Down
- Health of Standby CP. The Health of Standby CP can show one of the following values:

Healthy	The Standby CP is running and the background health diagnostic has not detected any errors.

Failed — The Standby CP is running, but the background health diagnostic has discovered a problem with the blade. The logs should be checked to determine the appropriate repair action. Fail-over will be disabled until the Standby CP can be repaired.

- HA Synchronization Status. The HA Synchronization Status field can show one of the following values:

  HA State Synchronized — The system is currently fully synchronized. If a fail-over were necessary at this time, the fail-over would be non-disruptive.

  HA State Not In Sync — The system is unable to synchronize the two CPs, due to the Standby CP being faulty or another system error. If a fail-over were to take place at this time, the Standby CP would be rebooted, and the fail-over will be disruptive.

Operands None

Example **To display control processor (CP) status:**

```
switch:admin> hashow
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
switch:admin>
```

See Also
- hadisable
- haenable
- hafailover
- hashow

hasyncstart

Enable the HA state synchronizing process.

Syntax `hasyncstart`

Availability Admin

Description Use this command to re-activate the HA State Synchronizing process.

Example **To enable the HA state synchronizing process:**

```
switch:admin> hasyncstart
HA State synchronization has started
switch:admin> hashow
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
switch:admin>
```

See Also `hasyncstop`
`hafailover`
`hashow`

hasyncstop

Disable the HA state synchronizing process.

Syntax `hasyncstop`

Availability Admin. This command is available only on the Active CP

Description Use this command to temporarily de-activate the HA Synchronization process.The next fail-over that takes place after may be disruptive as this command will deactivate the synchronization process.

Operands None

Example **To disable the HA state synchronizing process:**

```
Switch:admin> hasyncstop
Stop synchronize 0x228 (fabos):  Switch: 0, Info FSS_ME-FORCELOG, 4, HA State
   out of sync!
```

See Also `hasyncstart`

```
hafailover
hashow
```

help

Display help information for commands.

Syntax `help [command]`

Availability All users

Description Use this command without a operand to display an alphabetical list of commands. At the end of the list are additional commands that display groups of commands; for example `diaghelp` displays a list of diagnostic commands.

The list shows only commands that are available to the current user; this can vary according to:

- Login user level
- License key
- Switch model

To access help information for a specific command, enter the command name as an operand.

Operands This command has the following operand:

command	Specify the command name, with or without quotation marks. This operand is optional.

Example **To obtain help information on the password command:**

```
switch:admin> help passwd
```

See Also

```
diaghelp
licensehelp
routehelp
fwhelp
tshelp
zonehelp
perfhelp
```

historylastshow

Display last history record.

Syntax `historylastshow`

Availability All users

Description Use this command to display the contents of the last history log record. A history record contains three lines of information:

The first line of each record contains the following data sets:

- object type: CHASSIS, FAN, POWER SUPPLY, SW BLADE (switch), CP BLADE (control processor), WWN (world wide name), or UNKNOWN.
- object number: Slot <nn> (for blades), Unit <nn> (for everything else).
- event: Inserted, Removed, or Invalid.
- time of the event: at <Day> <Mon> <dd> <hh:mm:ss> <yyyy>

The second and third lines of a record each contain one data set, preceded by its name:

Factory Part Number: <xx-yyyyyyy-zz> or Unknown

Factory Serial Number: <xxxxxxxxxxxx> or Unknown

Operands None

Example **To display the last history record:**

```
switch:admin> historylastshow

CP BLADE  Slot 5         Inserted at Fri Feb  7 19:11:26 2003
Factory Part Number:     60-0001624-04
Factory Serial Number:   FP01X602ABA

Records:  100
switch:admin>
```

See Also `historyshow`

historymode

Display or set the mode of the history log

Syntax `historymode [mode]`

Availability Root / Factory (Set)

All users (Display)

Description Use this command to display or set the mode (as rotating or first-in) of the history buffer.

The history log buffer can have two modes of accepting new entries after it has reached its maximum size:

- Rotating mode: where new messages overwrite the oldest messages in the log.
- First-in mode: where once the log is full, all additional logs are discarded, so that the first set of logs to fill the buffer are preserved.

This command enables you to display the current history log mode and change between them. It also enables you to clear the history log buffer whenever the mode is changed.

This command, with no operand, displays the current history mode value.

This command, with an operand specified, sets the history mode to the new value.

Operands This command has the following operand:

mode	Specify `rot` for a rotating buffer, or `fi` for First-in mode. This operand is optional.

Example The following command sequence changes the history mode to first-in from rotating:

```
switch:admin> historymode
History Mode is: Rotating.
```

See Also

```
historyshow
historylastshow
```

historyshow

Display the history log.

Syntax `historyshow`

Availability All users

Description Use this command to display the history log. Each history record contains three lines of information:

1. The first line of each record contains the following data sets:
   - object type: CHASSIS, FAN, POWER SUPPLY, SW BLADE (switch), CP BLADE (control processor), WWN (world wide name), or UNKNOWN.
   - object number: Slot <nn> (for blades), Unit <nn> (for everything else).
   - event: Inserted, Removed, or Invalid.
   - time of the event: at <Day> <Mon> <dd> <hh:mm:ss> <yyyy>
2. The second contains one data set, Factory Part Number:
   - Factory Part Number: <xx-yyyyyyy-zz> or Unknown
3. The third line contains one data set, Factory Serial Number:
   - Factory Serial Number: <xxxxxxxxxxxx> or Unknown

Operands None

Example To display the entire contents of the history file:

```
switch:admin> historyshow

WWN  Unit 1              Inserted at Mon Feb  3 19:46:56 2003
Factory Part Number:     60-0001501-04
Factory Serial Number:   FT02X804F84

CP BLADE  Slot 5         Removed at Fri Feb  7 16:44:52 2003
Factory Part Number:     60-0001624-04
Factory Serial Number:   FP01X602ABA

CP BLADE  Slot 5         Inserted at Fri Feb  7 18:28:23 2003
Factory Part Number:     60-0001624-04
Factory Serial Number:   FP01X602ABA

CP BLADE  Slot 6         Inserted at Fri Feb  7 18:36:02 2003
Factory Part Number:     60-0001624-04
Factory Serial Number:   FP01X602964

CP BLADE  Slot 6         Inserted at Fri Feb  7 19:00:24 2003
Factory Part Number:     60-0001624-04
Factory Serial Number:   FP01X602964

Records:  5
switch:admin>
```

See Also `historylastshow`

httpcfgshow

Display the Java plug-in version.

Syntax `httpcfgshow`

Availability All users

Description Use this command to display the version of the Java plug-in supported by Web Tools. This command also displays the URL from where the plug-in can be downloaded.

Operands None

Example Display the Java plug-in version:

```
switch:admin> httpcfgshow
Current HTTP configuration
javaplugin.version = 1,3,1
javaplugin.homeURL = http://java.sun.com/products/plugin
```

i

Display task summary.

Syntax `i [Process ID]`

Availability All users

Description Use this command to display information of all of the processes or of a specific process if a process ID is supplied. One line is displayed per process. Table 1-10 explains the fields displayed with this commands.

Table 1-10 i Command Field Description

Field	Description
F	Process Flags: ALIGNWARN 001 print alignment warning messages STARTING 002 being created EXITING 004 getting shut down PTRACED 010 set if ptrace (0) has been called TRACESYS 020 tracing system calls FORKNOEXEC 040 forked but didn't exec SUPERPRIV 100 used super-user privileges DUMPCORE 200 dumped core SIGNALED 400 killed by a signal
S	Process state codes: D uninterruptible sleep (usually IO) R runnable (on run queue) S sleeping T traced or stopped Z a defunct (*zombie*) process
UID	The effective user ID number of the process.

Table 1-10 i Command Field Description (*continued*)

Field	Description
PID	The process ID of the process.
PPID	The process ID of the parent process.
C	Processor utilization for scheduling.
PRI	Priority number of the process. Higher numbers mean lower priority.
NI	Nice value used in priority computation.
ADDR	Memory address of the process.
SZ	The total size of the process in virtual memory in pages.
WCHAN	The address of an event for which process is sleeping (if blank, the process is running.).
TTY	The controlling terminal of the process (? is printed for no controlling terminal).
TIME	The cumulative execution time for the process.
CMD	The command name of the process.

Operands This command has the following operand:

taskId Specify the task name or task ID for the task to be displayed.

Example **To display information about process ID 433:**

```
switch:admin> i 433
F   S   UID   PID  PPID  C PRI  NI ADDR    SZ  WCHAN TTY   TIME     CMD
000 S     0   433     1  0  69   0    -  1283   5c64 ?   00:00:02 fabricd
switch:admin>
```

See Also `diaghelp`
`routehelp`

ifmodeset

Set the link operating mode for a network interface.

Syntax `ifmodeset ["interface"]`

Availability Admin

Description Use this command to set the link operating mode for a network interface.

An operating mode is confirmed with a `y` or `yes` at the prompt. If the operating mode selected differs from the current mode, the change is saved and the command exits.

Changing the link mode is not supported for all network interfaces or for all ethernet network interfaces. This command is only functional for the `eth0` interface.

Exercise care when using this command. Forcing the link to an operating mode not supported by the network equipment to which it is attached may result in an inability to communicate with the system through its ethernet interface.

For dual-CP systems, the `ifmodeset` command affects the CP that you are currently logged into. To set the link operating mode on the active CP you must issue this command on the active CP. To set the link operating mode on the standby CP you must issue this command on the standby CP. During failover the link operating mode is retained separately for each CP, since the physical links may be set to operate in different modes.

Operands This command has the following operand:

interface	Specify the name of the interface. You may specify the name with quotation marks, but using them is not required. For example, `"eth0"` or `eth0` where `eth` is the network interface and `0` is the physical unit.

Example To advertise all modes of operation, follow this scenario for the `ifmodeset` command:

```
switch:admin> ifmodeset eth0

Exercise care when using this command.  Forcing the link to
an operating mode not supported by the network equipment to
which it is attached may result in an inability to
communicate with the system through its ethernet interface.

It is recommended that you only use this command from the
serial console port.

Are you sure you really want to do this? (yes, y, no, n): [no] y
Proceed with caution.
Auto-negotiate (yes, y, no, n): [no] y
Advertise 100 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 100 Mbps / Half Duplex (yes, y, no, n): [yes] y
Advertise 10 Mbps / Full Duplex (yes, y, no, n): [yes] y
Advertise 10 Mbps / Half Duplex (yes, y, no, n): [yes] y
Committing configuration...done.
switch:admin>
```

To force 10 Mbps Half Duplex, follow this scenario for the `ifmodeset` command:

```
switch:admin> ifmodeset eth0

Exercise care when using this command.  Forcing the link to
an operating mode not supported by the network equipment to
which it is attached may result in an inability to
communicate with the system through its ethernet interface.

It is recommended that you only use this command from the
serial console port.

Are you sure you really want to do this? (yes, y, no, n): [no] y
Proceed with caution.
Auto-negotiate (yes, y, no, n): [no] n
Force 100 Mbps / Full Duplex (yes, y, no, n): [no]
Force 100 Mbps / Half Duplex (yes, y, no, n): [no]
Force 10 Mbps / Full Duplex (yes, y, no, n): [no]
Force 10 Mbps / Half Duplex (yes, y, no, n): [no] y
Committing configuration...done.
switch:admin>
```

See Also `ifmodeshow`

ifmodeshow

Display the link operating mode for a network interface.

Syntax `ifmodeshow ["interface"]`

Availability All users

Description Use this command to display the link operating mode for a network interface.

Operands This command has the following operand:

interface	Specify the name of the interface. You may specify the name with quotation marks, but using them is not required. For example, `"eth0"` or `eth0` where `eth` is the network interface and `0` is the physical unit.

Example **To display the link operating mode for the "eth0" ethernet interface:**

```
switch:admin> ifmodeshow "eth0"
Link mode: negotiated 100baseTx-HD, link ok
switch:admin>
```

See Also `ifmodeset`

interfaceshow

Display FSPF interface information.

Syntax `interfaceshow [slot_number/] [port_number]`

Availability All users

Description Use this command to display data structures associated with FSPF interfaces (E_Ports) on the switch.

There are two data structures that save data associated with FSPF interfaces:

- the permanently allocated Interface Descriptor Block (IDB)

- the neighbor data structure. This data structure is allocated when a switch port becomes an E_Port. The neighbor data structure contains all the information relating to the switch that is connected to an adjacent switch.

This command displays the content of both data structures, if they have been allocated.

Use this command without specifying a port number to display the interface information for all ports on the switch (including non E_Ports).

The following fields are displayed:

idbP	Pointer to IDB.
nghbP	Pointer to neighbor data structure.
ifNo	Interface number.
masterPort	Port number of the trunk master port, if present, of the trunk group this port is a part of.
defaultCost	The default cost of sending a frame over the ISL connection to this interface.
cost	Cost of sending a frame over the ISL connected to this interface. A value of 1000 indicates a 1 Gbit/sec link. A value of 500 indicates a 2 Gbit/sec link.
delay	Conventional delay incurred by a frame transmitted on this ISL. A fixed value required by the FSPF protocol.
lastScn	Type of the last State Change Notification received on this interface.
lastScnTime	Time the last State Change Notification was received on this interface.
upCount	Number of times this interface came up, with respect to FSPF.
lastUpTime	Last time this interface came up.
downCount	Number of times this interface went down.
lastDownTime	Last time this interface went down.
downReason	Type of last State Change Notification that caused this interface to go down.

iState	Current state of this interface. The state can be UP or DOWN. An interface in DOWN state does not have an allocated neighbor data structure and cannot be used to route traffic to other switches.
state	Current state of this interface. This E_Port is used to route traffic to other switches only if the state is 'NB_ST_FULL'.
nghbCap	Neighbor capabilities. Should be 0.
nghbId	Domain ID of the neighbor (adjacent) switch.
idbNo	IDB number. Should be equal to portnumber
remPort	Port number on the remote switch connected to this port.
nflags	Internal FSPF flags.
initCount	Number of times this neighbor was initialized, without the interface going down.
&dbRetransList	Pointer to the database retransmission list.
&lsrRetransList	Pointer to the Link State Records (LSR) retransmission list.
&lsrAckList	Pointer to the Link State Acknowledgements (LSA) retransmission list.
inactTID	Inactivity timer ID.
helloTID	Hello timer ID.
dbRtxTID	Database retransmission timer ID.
lsrRtxTID	LSR retransmission timer ID.
inactTo	Inactivity time out value, in milliseconds. When this time out expires, the adjacency with the neighbor switch is broken and new paths are computed to all possible destination switches in the fabric.
helloTo	Hello time out value, in milliseconds. When this time out expires, a Hello frame is sent to the neighbor switch through this port.
rXmitTo	Retransmission time out value, in milliseconds. It is used to transmit topology information to the neighbor switch. If no acknowledgement is received within rXmitTo, frame is retransmitted.

nCmdAcc	Total number of commands accepted from the neighbor switch. Number includes Hellos, Link State Updates (LSU) and Link State Acknowledgements.
nInvCmd	Number of invalid commands received from the neighbor switch. Usually commands with an FSPF version number higher than the one running on the local switch.
nHloIn	Number of Hello frames received from the neighbor switch.
nInvHlo	Number of invalid Hello frames (Hello frames with invalid parameters) received from the neighbor switch.
nLsuIn	Number of LSUs received from the neighbor switch.
nLsaIn	Number of LSAs received from the neighbor switch.
attHloOut	Number of attempted transmissions of Hello frames to the neighbor switch.
nHloOut	Number of Hello frames transmitted to the neighbor switch.
attLsuOut	Number of attempted transmissions of LSUs to the neighbor switch.
nLsuOut	Number of LSUs transmitted to the neighbor switch.
attLsaOut	Number of attempted transmissions of LSAs to the neighbor switch.
nLsaOut	Number of LSAs transmitted to the neighbor switch.

Operands This command has the following operands:

slot_number	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number

5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

port_number Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

When no slot number and port number are specified, this command displays the interface information for all ports on the switch (including non E_Ports).

Examples

To display FSPF interface information:

```
switch:admin> interfaceshow 9/1

idbP            = 0x1007f558

Interface 33 data structure:

nghbP           = 0x10080658
ifNo            = 33
masterPort      = 33 (self)
defaultCost     = 1000
cost            = 500
delay           = 1
lastScn         = 5
lastScnTime     = Mar 05 08:59:27.180
upCount         = 1
lastUpTime      = Mar 05 08:59:27.180
downCount       = 0
lastDownTime    = Jan 01 00:00:00.000
downReason      = 0
iState          = UP


Type <CR> to continue, Q<CR> to stop:
```

See Also

portshow
switchshow

interopmode

Enables or disables Brocade switch interoperability with switches from other manufacturers.

Syntax `interopmode [mode]`

Availability Admin

Description Use this command to enable or disable interoperability mode for individual Brocade switches. This feature enables other manufacturers' switches to be used in a Brocade fabric.

This command must be executed on all Brocade switches in the fabric. The switch must be rebooted after changing interoperability mode. In a heterogeneous fabric, several Brocade features are not available in order to provide maximum compatibility between switches.

Brocade domain IDs must be in the 97 to 127 value range for successful connection to other switches. The firmware automatically assigns a valid domain ID, if necessary, when interoperability mode is enabled on the switch.

Before enabling interoperability mode, the individual fabrics should be inspected for compatibility. Zones should be inspected to ensure that they meet the zone criteria and restrictions. Remove or disable any unsupported optional features. Disable the Platform Management functions using the `msplmgmtdeactivate` command.

When the switch is running within interoperability mode, the following normally configurable selections will be pre-set to values required by the interoperability mode, and they will also no longer be changeable using the `configure` command:

- Domain ID: Only valid inputs range from 97 to 127.
- Port no. zoning: Will be disabled.
- Node WWN zoning: Will be disabled.
- QL zoning: Will be disabled.
- VC encoded address: Will be disabled.
- Secure Fabric OS: Will be disabled.

When the interoperability mode is disabled, the above configuration parameters will be reset back to their DEFAULT state. They will also once again be changeable using the `configure` command.

When you are in interopmode, the only type of zoning supported is port WWN zoning. That means using the device's port WWN, for example, 10:00:00:00:c9:28:c7:c6.

Zone configurations that use either physical port numbers or port IDs are not supported in interopmode. Zoning using port number uses the actual physical port numbers on the switch, for example slot 1, port 5. Zoning using port ID uses the device ID, for example, 010100.

Interoperability mode places considerable restrictions upon the features of a fabric. For detailed information on restrictions associated with interoperability mode, refer to the Enabling Interoperability Mode chapter in the *Fabric OS Procedures Guide*.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands

This command has the following operand:

mode	Specify 1 to enable interoperability mode; specify 0 to disable interoperability mode. This operand is optional.

If no operand is specified the current value is displayed.

Example

To view and then enable interoperability mode:

```
switch:admin> interopmode
InteropMode: Off

Usage: InteropMode 0|1
         0: to turn it off
         1: to turn it on
switch:admin> interopmode 1
done.
Interopmode is enabled.
switch:admin> reboot
```

See Also

`configure`

iodreset

Turn off the In-order Delivery (IOD) option.

Syntax `iodreset`

Availability Admin

Description Use this command to turn off the IOD option. The IOD option is turned off by default. If the IOD option was turned on using `iodset`, this command can be used to turn it off again. Setting the IOD option to its default value will result in fast re-routing after a fabric topology change.

This command may cause out-of-order delivery of frames during fabric topology changes.

Operands None

Examples **To turn off the IOD option:**

```
switch:admin> iodreset
done.
switch:admin>
```

See Also

```
iodset
iodshow
```

iodset

Enable the In Order Delivery (IOD) option.

Syntax `iodset`

Availability Admin

Description Use this command to enforce in order delivery of frames during a fabric topology change.

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, generally, some frames are delivered out of order. This command insures that frames are not delivered out-of-order, even during fabric topology changes.

The default behavior is for the IOD option to be off.

This command should be used with care, because it can cause a delay in the establishment of a new path when a topology change occurs. Only if there are devices connected to the fabric that do not tolerate occasional out of order delivery of frames, should this command be used.

Operands None

Examples **To turn on the IOD option:**

```
switch:admin> iodset
done.
switch:admin>
```

See Also

```
iodreset
iodshow
```

iodshow

Display the In Order Delivery (IOD) option setting.

Syntax

```
iodshow
```

Availability All users

Description Use this command to display whether the IOD option is enabled or disabled.

Operands None

Example **To display the current setting of the IOD option:**

```
switch:admin> iodshow

IOD is not set

switch:admin>
```

See Also

```
iodset
iodreset
```

ipaddrset

Set the IP Address details for a switch or control processor.

Syntax `ipaddrset [option]`

Availability Admin

Description Use this command to set the Ethernet and Fibre Channel IP addresses on the switch.

For a ED-12000B, you must set values for both logical switches and both CP cards. Use the *option* operand to select the logical switch or CP where you want to configure an IP address. The *option* operand is only available for the ED-12000B. If the *option* operand is not specified for a ED-12000B, the command becomes interactive.

Each logical switch has:

- Ethernet IP Address
- Ethernet Subnetmask
- Fibre Channel IP Address
- Fibre Channel Subnetmask

Each CP has:

- Ethernet IP Address
- Ethernet Subnetmask
- Host Name
- Gateway IP Address

The default values for hostname, ipaddress, subnet address (for CP only), mask (for switch only), and gateway address (for CPs only) are:

- sw0 = hostname SW12000_1, ip 10.77.77.77, mask 255.0.0.0
- sw1 = hostname SW12000_2, ip 10.77.77.76, mask 255.0.0.0
- cp0 = hostname cp0, ip 10.77.77.75, subnet 255.0.0.0, gateway 0.0.0.0
- cp1 = hostname cp1, ip 10.77.77.74, subnet 255.0.0.0, gateway 0.0.0.0

Entering Values and Saving Changes After each prompt the current value is shown. You may:

- Press RETURN to retain the current value

- Enter an IP address in conventional dot notation
- Enter `none`
- Press CONTROL-C to cancel changes
- Press CONTROL-D to accept changes and end input

The final prompt enables you to set the new IP addresses immediately. Enter Y to set new addresses immediately; enter N to delay the changes until the next switch reboot. Entering Y closes the telnet session.

A change to these values issues a domain address format RSCN, refer to FC-FLA for a description of RSCNs.

Operands This command has the following operand:

option Specify which option you would like to configure. This operand is only available for the ED-12000B. Valid options are as follows:

- `0` sets the Ethernet IP Address, Ethernet Subnetmask, Fibre Channel IP address and Fibre Channel Subnetmask of logical switch 0.
- `1` sets the Ethernet IP Address, Ethernet Subnetmask, Fibre Channel IP address and Fibre Channel Subnetmask of logical switch 1.
- `2` sets the Ethernet IP Address, Ethernet Subnetmask, gateway IP address and Hostname of CP0.
- `3` sets the Ethernet IP Address, Ethernet Subnetmask, gateway IP address and Hostname of CP1.

If no operand is specified the command becomes interactive.

Example **To set the IP address details for logical switch number 1 in an ED-12000B:**

```
switch:admin> ipaddrset 1
Ethernet IP Address [10.77.77.77]: 123.123.123.123
Ethernet Subnetmask [10.77.77.76]: 123.123.123.124
Fibre Channel IP Address [0.0.0.0]: 123.123.123.125
Fibre Channel Subnetmask [0.0.0.0]: 123.123.123.126
IP address being changed...
Committing configuration...Done.
switch:admin>
```

To set the IP address details for a DS-32B2:

```
switch:admin> ipaddrset
Ethernet IP Address [10.77.77.77]: 123.123.123.123
Ethernet Subnetmask [10.77.77.76]: 123.123.123.124
Fibre Channel IP Address [0.0.0.0]:
Fibre Channel Subnetmask [0.0.0.0]:
Gateway IP Address [10.64.112.1]:
IP address being changed...
Committing configuration...Done.
switch:admin>
```

See Also `ipaddrshow`

ipaddrshow

Display the IP address information for a switch or control processor.

Syntax `ipaddrshow [option]`

Availability All users

Description Use this command to display the Ethernet and FC IP addresses configured in the system.

The *option* operand is only available on the ED-12000B. This operand is not available on the DS-32B2.

For a switch, this command displays the following details: Ethernet IP Address, Ethernet Subnetmask, Fibre Channel IP Address, and Fibre Channel Subnetmask.

For a CP, this command displays the following details: Ethernet IP Address, Ethernet Subnetmask, Hostname and Gateway IP address.

In the ED-12000B the CPs communicate to each other through an Ethernet in the backplane. When the *option* operand is specified as a 4, the fixed Backplane IP addresses for CP0 and CP1 are also shown.

Use the *option* operand to specify the logical switch or CP you want to view. If the option operand is not specified, then the command becomes interactive.

The default values for hostname, IP address, subnet address (for CP only), mask (for switch only), and gateway address (for CPs only) are:

- sw0 = hostname SW12000_1, ip 10.77.77.77, mask 255.0.0.0

- sw1 = hostname SW12000_2, ip 10.77.77.76, mask 255.0.0.0
- cp0 = hostname cp0, ip 10.77.77.75, subnet 255.0.0.0, gateway 0.0.0.0
- cp1 = hostname cp1, ip 10.77.77.74, subnet 255.0.0.0, gateway 0.0.0.0

Operands

This command has the following operand:

option — Specify the option you would like to view. This operand is only available for the ED-12000B. Valid option values are:

- 0 means display information for switch0.
- 1 means display information for switch1.
- 2 means display information for cp0.
- 3 means display information for cp1.
- 4 means display information all IP addresses in the system.

If no operand is specified the command becomes interactive.

Example

To display the IP address for logical switch 0 in an ED-12000B:

```
switch:admin> ipaddrshow 0
Ethernet IP Address: 123.123.123.123
Ethernet Subnetmask: 123.123.123.124
Fibre Channel IP Address: 0.0.0.0
Fibre Channel Subnetmask: 0.0.0.0
switch:admin>
```

To display the IP address information for a DS-32B2:

```
switch:admin> ipaddrshow
Ethernet IP Address: 123.123.123.123
Ethernet Subnetmask: 123.123.123.124
Fibre Channel IP Address: 0.0.0.0
Fibre Channel Subnetmask: 0.0.0.0
Gateway Address: 123.123.123.125
switch:admin>
```

See Also

`ipaddrset`

islshow

Displays ISL information.

Syntax `islshow`

Availability All users

Description Use this command to display the current connections and status of the ISL of each port on this switch. The WWN where the ISL is connected to, the speed of the connection, and whether this ISL is trunked, are displayed.

Operands None

Example **To display the ISL connections for the switch:**

```
switch:admin> islshow
1: 33 -> 29   10:00:00:60:69:80:4f:84 switch sp: 2G  bw: 4G  TRUNK
2: 39 ->  7   10:00:00:60:69:80:4f:84 switch sp: 2G  bw: 8G  TRUNK
3: 41 ->  (incompatible)
4: 47 ->  (incompatible)
5: 57 -> 25   10:00:00:60:69:80:4f:84 switch sp: 2G  bw: 4G  TRUNK
6: 60 ->  2   10:00:00:60:69:80:4f:84 switch sp: 2G  bw: 4G  TRUNK
switch:admin>
```

See Also `switchshow`

itemlist

List parameter syntax and grammar information.

Syntax

```
<item_list> = <element> | <element> <white> <item_list>
<element>   = <item> | <item> - <item>
<item>      = <num> | <slot> [ <white> ] / [ <white> ]
<num>
<slot>      = <num>
<num>       = <hex> | <int>
<int>       = <int> <digit> | <digit>
<hex>       = 0x <hex digit> | <hex> <hex digit>
<digit>     = 0|1|2|3|4|5|6|7|8|9
```

```
<hex digit> = <digit> |A|B|C|D|E|F|a|b|c|d|e|f
<white>     = *["\t\f\r ,"]
```

Description

All kernel diagnostics have at least one item list parameter to specify which ports to test. The normal default value for this parameter is to select everything.

This is not a command, rather it is a common parameter to many commands.

If you wish to restrict the items to be tested to a smaller set the parameter value is an item list with the following characteristics:

- It is a comma separated list of items.
- Each item in the list may be a single element or a range of elements separated with a - character.
- white space like spaces, and tab stops are skipped.
- ranges using - can be mixed with individual values.
- Each item may be proceeded by an optional slot number and /. for example `0,3,4-6,1, 0,1,3,4,5,6,0 3 4 - 6 1` will all select items 0, 1, 3, 4, 5, 6 and 7.

Besides the syntax rules, there are also some grammatical restrictions on the slot numbers:

- Once specified a slot selection will apply to all following items to the right of the slot selection until the next slot selection or the end of the item list. For example, `1/0 - 15` and `1/0 - 1/15` are equivalent.
- If no slot number is specified then User port lists will be specified by area number. For instance `0, 16, 32` and `1/0, 2/0, 3/0` specify the same ports on a 16 port/blade system. On that same system `1/0, 16, 32` is not a legal list. Even though it is legal syntax the ports do not exist.
- If no slot number is specified then all lists except user port lists will use the default slot 0.
- No list type except for user port lists may specify multiple conflicting slot numbers. For instance `1/0, 2/0, 3/0` is a legal user port list but is not legal for any other type of list.

- In the case of conflicting settings within a single itemlist an error will be generated as described above. In the case of multiple item list parameters, the last one on the command line will override any previous settings.

The exact type of list varies depending on the test and the parameter but the most common are Blade ports and User ports. A list of blade ports is most commonly used by the ASIC level tests such as cmitest or turboramtest and represents which ports on the current blade (specified with --slot # parameter) will be tested. A list of user ports is used by the higher level tests such as spinsilk or crossporttest to specify which user accessible external ports within the current switch (selected during telnet login) will be tested. When specified in an item list user ports may be specified by either the area portion of the ports fibre channel address or with slot/port notation. For non-bladed systems the port number on the silkscreen is the area number so the two notations are identical.

The exact type of list required for any input parameter may be determined with the `diagcommandshow` <test> command. For item list parameters the parameter type will be PT_LIST and the list type will be one of the following shown in Table 1-11:

Table 1-11 Object Descriptions

Type	Grouping	Description
BPORTS	Blade	Blade ports, internal and external ports.
UPORTS	Switch	User ports, ports with external connections.
QUADS	Blade	Quadrants, group of (normally 4) ports.
CHIPS	Blade	Chips, Asics within a blade.
MINIS	Blade	Mini switches.
SLOTS	Chassis	Slots.
INDEX	N/A	Anything.

See Also

```
diagcommandshow
portregtest
centralmemorytest
cmitest
camtest
portloopbacktest
sramretentiontest
```

```
cmemretentiontest
crossporttest
backport
spinsilk
```

killtelnet

Terminate an open telnet session.

Syntax `killtelnet`

Availability Admin

Description Use this command to terminate an open telnet session. The `killtelnet` command is an interactive menu driven command. Upon invocation, it lists all the current telnet and serial port login sessions. It lists information such as the session number, login name, the idle time, the IP address of the connection, and the time stamp of when the login session was opened. A prompt is then displayed where you can specify the session number of the connection you wish to terminate.

Example To terminate an open telnet connection:

```
switch:admin> killtelnet

Collecting login information....Done

                  List of telnet sessions (3 found)

 Session No   USER         TTY          IDLE        FROM              LOGIN@
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     0        root0        ttyS0         1:17m       -                 5:13pm
     1        admin0       pts/0        16.00s       192.168.130.29    6:29pm
     2        admin0       pts/1         3.00s       192.168.130.29    6:31pm
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

 Enter Session Number to terminate (q to quit) 1
Collecting process information... Done.

        You have opted to terminate the telnet session:-
                logged in as "admin0 ", from "192.168.130.29 "
                since " 6:29pm" and has been inactive for "16.00s ",
                the current command executed being: "-rbash ".
                The device entry is: "pts/0 ".

        This action will effectively kill these process(es):-
                      USER        PID ACCESS COMMAND
/dev/pts/0            root      12868 f....  login
                      root      12869 f....  login
                      root      12877 f....  rbash
Please Ensure (Y/[N]): y
killing session....  Done!

Collecting login information....Done

                  List of telnet sessions (2 found)

 Session No   USER         TTY          IDLE        FROM              LOGIN@
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     0        root0        ttyS0         1:17m       -                 5:13pm
     1        admin0       pts/1         7.00s       192.168.130.29    6:31pm
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

 Enter Session Number to terminate (q to quit) q
switch:admin>
```

The list of open sessions displayed with killtelnet includes the user's current session. Make sure you do not kill your own telnet session.

licenseadd

Add license key to switch.

Syntax `licenseadd "license"`

Availability Admin

Description Use this command to add license keys to the system.

Some features of the switch and of the fabric to which it is connected are optional licensed products. Without a license installed for such products, the services are not available.

A license key is a string of approximately 16 upper and lower case letters and numbers. Case is significant.

The license must be entered into the system exactly as issued. If entered incorrectly, the license may be accepted, but the licensed products will not function. After entering the license, use the `licenseshow` command to check for correct function. If no licensed products are shown, then the license is invalid.

After entering a license, the licensed product is available immediately and the system does not need to be rebooted. There is an exception. For a trunking license to become effective, the trunk ports need to be refreshed using the commands `portdisable` and `portenable` or the switch must be refreshed using the commands `switchdisable` and `switchenable`. A QuickLoop only system must be rebooted after adding a fabric license to allow fabric logins.

Operands This command has the following operand:

license	Specify a license key in quotation marks. This operand is required.

Example **To add a license key to the switch:**

```
switch:admin> licenseadd "aBcDeFGh12345"
adding license key "aBcDeFGh12345"
done.
```

See Also

`licenseremove`
`licenseshow`

licensehelp

Display commands used to administer license keys.

Syntax `licensehelp`

Availability All users

Description Use this command to display a list of the commands used to administer license keys.

Operands None

Example **To display license commands:**

```
switch:admin> licensehelp

licenseAdd              Add a license to this switch
licenseIdShow           Show system license ID
licenseRemove           Remove a license from this switch
licenseShow             Show current licenses

switch:admin>
```

See Also
`licenseadd`
`licenseidshow`
`licenseremove`
`licenseshow`

licenseidshow

Display system license ID.

Syntax `licenseidshow`

Availability All users

Description Use this command to display the license ID of a DS-32B2 or a ED-12000B chassis.

Some features of the switch and the fabric are optional, licensed products. Without a license installed for such products, the services provided by these features are not available.

For the ED-12000B a single license enables both logical switches to use these products. That is, the chassis is assigned a license ID from which a license is generated.

Such licenses are locked and are only functional on the specific system for which they were issued.

This command displays to standard output the system license ID used for both generating and validating licenses on the system. The license ID format is 8 pairs of hexidecimal values separated by colons. Each hexidecimal value is between 00 (0) and FF (255).

While the format of this identifier may be similar or identical to other identifiers in the system, no inferences should be made about the relationships between them as they are subject to change independent of one another.

Operands None

Example **To display the license ID:**

```
switch:admin> licenseidshow
a4:f8:69:33:22:00:ea:18
```

See Also

```
licenseadd
licensehelp
licenseremove
licenseshow
```

licenseremove

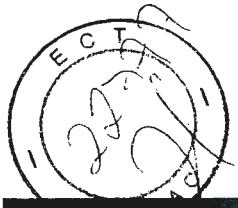
Remove the license key from a switch.

Syntax `licenseremove "license"`

Availability Admin

Description Use this command to remove an existing license key from a switch. The existing license key must be entered exactly as shown by `licenseshow`, including case.

When the key has been entered, use the `licenseshow` command to verify that the key has been removed and the licensed product un-installed.



After removing a license key, the switch must be rebooted. With no license key, `licenseshow` displays "No licenses".

Operands The following operand is required:

license	Specify the license key in quotation marks. This operand is required.

Example **To remove a license key from the switch:**

```
switch:admin> licenseremove "aBcDeFGh12345"
removing license-key "aBcDeFGh12345"
Committing configuration...done.
For license to take effect, Please reboot switch now....
switch:admin>
```

See Also
```
licenseadd
licensehelp
licenseidshow
licenseshow
```

licenseshow

Display current license keys.

Syntax `licenseshow`

Availability All users

Description Use this command to display current license keys along with a list of licensed products enabled by these keys. The message `No license installed on this switch` is displayed when no licenses are installed.

Operands None

Example **To display the installed license keys on a switch:**

```
switch:admin> licenseshow
aBcDeFGh12345:
    Web license
    Zoning license
    Remote Switch license
    Remote Fabric license
    Extended Fabric license
    Fabric Watch license
    Performance Monitor license
```

```
    Trunking license
    Security license
switch:admin>
```

See Also

```
licenseadd
licensehelp
licenseidshow
licenseremove
```

linkcost

Set or print the FSPF cost of a link.

Syntax `linkcost [slotnumber/][portnumber][, cost]`

Availability Admin

Description Use this command to set or display the cost of an Inter-Switch Link (ISL). The cost of a link is a dimensionless positive number. It is used by the FSPF path selection protocol to determine the path that a frame takes going from the source to the destination switch. The chosen path is the path with minimum cost. The cost of a path is the sum of the costs of all the ISLs traversed by the path. The cost of a path is also known as the *metric*.

FSPF supports load sharing over a number of equal cost paths.

Every ISL has a default cost that is inversely proportional to the bandwidth of the ISL. For a 1 Gbit/sec per second ISL, the default cost is 1000. For a 2 Gbit/sec ISL, the default cost is 500

All currently active ISLs have an additional suffix of E_PORT attached to their interface numbers. If the link has a static cost assigned to it, then the link cost for that link has a suffix of STATIC attached to its link cost.

This command changes the actual link cost only; it does not affect the default cost. The `interfaceshow` command displays both the default and the actual cost.

If no operands are specified, the command displays the actual cost of all the ISLs in the (logical) switch. Specify the `[slotnumber/]portnumber` operand to view the *cost* of that specific port. Specify `[slotnumber/]portnumber` and `cost` operand to set the cost of a specific ISL.

Setting the cost to zero removes a static cost from the database and reverts the cost of the link to its default value.

Operands

This command has the following operands:

slotnumber — Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber — Specify the port to display or set the FSPF cost of a link. Valid values for port number vary depending on the switch type. This operand is optional.

cost — Specify the new cost of the link connected to the specified port number. This operand is optional.

If no operands are specified, the current values for all ports on the (logical) switch are displayed.

Example

To display the cost of a link, and reset the cost:

```
switch:admin> linkcost
  9/0              500
  9/1 (E_PORT)     500
  9/2              500
  9/3              500
  9/4              500
  9/5              500
  9/6              500
  9/7 (E_PORT)     500
  9/8              500
  9/9 (E_PORT)    1000
  9/10             500
  9/11             500
  9/12             500
  9/13             500
  9/14             500
  9/15 (E_PORT)   1000

--- <output truncated> ---
```

```
switch:admin> linkcost 9/1 1000
done.
switch:admin>
```

See Also

```
interfaceshow
lsdbshow
topologyshow
urouteshow
```

login

Login as new user

Syntax `login`

Availability All users

Description Use this command to login to the switch with another user name and password, without first logging out from the original session. If the user was originally connected using a telnet or rlogin session, that session is left open.

This command allows you to access commands that you cannot access at your current user level.

Operands None

Example **To login as admin from a user:**

```
switch:user> login
login: admin
Password:xxxxxx
switch:admin>
```

See Also `logout`

logout

Logout from a telnet, rlogin or serial port session.

Syntax `logout`

Availability All users

Description Use this command to logout from a telnet, rlogin or serial port session. Telnet and rlogin connections are closed, the serial port returns to the `login:` prompt.

The command `exit` is accepted as a synonym for `logout`, as is CONTROL-D entered at the beginning of a line.

If you close a telnet or sectelnet session by clicking the X in the upper right hand corner, the window closes but the session stays open until it times out. Trying to open another session before the time-out has completed causes an error message to display.

Operands None

Example **To log out from a rlogin session:**

```
switch:admin> logout
Connection to host lost.
```

See Also `login`

loopporttest

Functional test of L_port M->M path on a loop.

Syntax `loopporttest [-nframes` *`count`*`] [-ports` *`itemlist`*`] [-seed` *`payload_pattern`*`] [-width` *`pattern_width`*`]`

Availability Admin

Description Use this command to verify the operation of the switch by sending frames from port M's transmitter, and looping the frames back through an external fiber cable, including all the devices on the loop, into port M's receiver. This exercises all the switch components from the main board to the SFP to the fiber cable to the SFPs (of the devices and the switch) and back to the main board.

The cables and SFPs connected should be of the same technology: meaning a short wavelength SFPed (switch) port is connected to another short wavelength SFPed (device) port through a short wavelength cable; and a long wavelength port is connected to a long wavelength port; and a copper port is connected to a copper port.

Only one frame is transmitted and received at any one time. The port LEDs flicker green rapidly while the test is running.

The test method is as follows:

1. Determine which ports are L-ports.
2. Enable ports for cabled loopback mode.
3. Create a frame F of data size (1024 bytes).
4. Transmit frame F via port M, with D_ID to the FL port (ALPA = 0).
5. Pick up the frame from port M, the FL port.
6. Check if any of the 8 statistic error counters are non-zero: ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.
7. Check if the transmit, receive or class 3 receiver counters are stuck at some value.
8. Check if the number of frames transmitted is not equal to the number of frames received.
9. Repeat steps 3 through 8 for all ports present until:
   a. the number of frames requested is reached,
   b. all ports are marked bad.

You can specify a payload pattern to be used when executing this test. If the pattern is not specified, then at every 30 passes, a different data type is used to generate new pattern to create the frame. The data pattern will be generated base on each data type. Some data type may generate different data patterns on every pass. The data types are repeated every 210 pass.

Operands

This command has the following operands:

`-nframes` *`count`* Specify the number of times (or number of frames per port) to execute this test. The default value is 10.

`-ports` *`itemlist`* Specify a list of user ports to test. By default all the user ports in the current slot are tested. Refer to `itemlist` for more information on selecting ports.

`-seed` *`payload_pattern`*
Specify the seed pattern of the test packets. The data types are:

- 1. CSPAT: 0x7e, 0x7e, 0x7e, 0x7e, ...
- 2. BYTE_LFSR: 0x69, 0x01, 0x02, 0x05, ...
- 3. CHALF_SQ: 0x4a, 0x4a, 0x4a, 0x4a, ...
- 4. QUAD_NOT: 0x00, 0xff, 0x00, 0xff, ...
- 5. CQTR_SQ: 0x78, 0x78, 0x78, 0x78, ...
- 6. CRPAT: 0xbc, 0xbc, 0x23, 0x47, ...
- 7. RANDOM: 0x25, 0x7f, 0x6e, 0x9a, ...

`-width` *`pattern_width`*

Specify the width of the test pattern. Valid values include:

- 1 for byte
- 2 for word
- 3 for quad

This operand is optional.

Example

To perform a loopback port test:

```
switch:admin> loopporttest -ports 1/0-1/15

Running Loop Port Test .......
Test Complete: "loopporttest" Pass 10 of 10
Duration 0 hr, 0 min & 1 sec (0:0:0:127).
passed.
```

Errors

Below are possible error messages if failures are detected:

```
DATA
INIT
PORT_DIED
EPI1_STATUS_ERR
ERR_STAT
ERR_STATS
ERR_STATS_2LONG
ERR_STATS_BADEOF
ERR_STATS_BADOS
ERR_STATS_C3DISC
ERR_STATS_CRC
ERR_STATS_ENCIN
ERR_STATS_ENCOUT
ERR_STATS_TRUNC
ERR_STAT_2LONG
ERR_STAT_BADEOF
ERR_STAT_BADOS
ERR_STAT_C3DISC
ERR_STAT_CRC
ERR_STAT_ENCIN
ERR_STAT_ENCOUT
ERR_STAT_TRUNC
```

```
FDET_PERR
FINISH_MSG_ERR
FTPRT_STATUS_ERR
LESSN_STATUS_ERR
MBUF_STATE_ERR
MBUF_STATUS_ERR
NO_SEGMENT
PORT_ABSENT
PORT_ENABLE
PORT_M2M
PORT_STOPPED
PORT_WRONG
RXQ_FRAME_ERR
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FRX
STATS_FTX
TIMEOUT
XMIT
```

See Also

```
camtest
centralmemorytest
cmemretentiontest
cmitest
itemlist
portloopbacktest
portregtest
spinsilk
sramretentiontest
crossporttest
```

lsdbshow

Display the FSPF Link State Database.

Syntax `lsdbshow [domain]`

Availability All users

Description Use this command to display a FSPF Link State Database records for switches in the fabric.

There are two types of database entries:

- the Link State Database Entry, which is permanently allocated.
- the Link State Record (LSR) which is allocated when a switch is connected to the fabric.

The LSR describes the links between connected domains in a fabric. For a link to be reported in the LSR, the neighbor for that link must be in NB_ST_FULL state.

This command displays the content of both types of database entries, if both are present.

Without operands, this command displays the whole Link State Database.

The display shows the following fields shown in Table 1-12:

Table 1-12 lsdbshow Display Fields

Field	Description
Domain	Domain number described by this LSR. A (self) keyword after the domain number indicates LSR describes the local switch.
lsrP	Pointer to LSR.
earlyAccLSRs	Number of LSRs accepted even though they were not sufficiently spaced apart.
ignoredLSRs	Number of LSRs not accepted because they were not sufficiently spaced apart.
lastIgnored	Last time an LSR was ignored.
installTime	Time this LSR was installed in the database, in seconds since boot.
lseFlags	Internal variable.
uOutIfs	Internal variable
uPathCost	Internal variable.
uOldHopCount	Internal variable.
uHopsFromRoot	Internal variable.
mOutIfs	Internal variable.
parent	Internal variable.
mPathCos	Internal variable.
mHopsFromRoot	Internal variable.

Table 1-12 lsdbshow Display Fields *(continued)*

Field	Description
lsAge	Age, in seconds, of this LSR. An LSR is removed from the database when its age exceeds 3600 seconds.
reserved	Reserved for future use.
type	Type of the LSR. Always 1.
options	Always 0.
lsId	ID of this LSR. It is identical to the domain number.
advertiser	ID (domain number) of the switch that originated this LSR.
incarn	Incarnation number of this LSR.
length	Total length (in bytes) of this LSR. Includes header and link state information for all links.
chksum	Checksum of total LSR, with exception of `lsAge` field.
linkCnt	Number of links in this LSR. Each link represents a neighbor in NB_ST_FULL state.
flags	Always 0.
LinkId	ID of this link. It is the domain number of the switch on the other side of the link.
out port	Port number on the local switch.
rem port	Port number of the port on the other side of the link.
cost	Cost of this link. The default cost for a 1 Gbit/sec link is 1000.
costCnt	Always 0.
type	Always 1.

Operands This command has the following operand:

`domain` Specify the domain number of the LSR to be displayed. This operand is optional.

Examples

To display the link state record for the local switch:

```
switch:admin> lsdbshow

Domain = 1 (self), Link State Database Entry pointer = 0x10080230
lsrP              = 0x10081210
earlyAccLSRs      = 0
ignoredLSRs       = 0
lastIgnored       = Never
installTime       = 0x12dbd46 (19774790)
lseFlags          = 0xa
uOutIfsP[0]       = 0x00000000
uOutIfsP[1]       = 0x00000000
uPathCost         = 0
uOldHopCount      = 0
uHopsFromRoot     = 0
mOutIfsP[0]       = 0x00000000
mOutIfsP[1]       = 0x00000002
parent            = 0xf0
mPathCost         = 0
mHopsFromRoot     = 0

Link State Record:
Link State Record pointer = 0x10081210
lsAge             = 151
reserved          = 0
type              = 1
options           = 0x0
lsId              = 1
advertiser        = 1
incarn            = 0x80000010
length            = 92
chksum            = 0xa58f
linkCnt = 4,      flags = 0x0
LinkId =   2, out port =  33, rem port =  29, cost = 1000, costCnt = 0, type
   = 1
LinkId =   2, out port =  39, rem port =   7, cost = 500, costCnt = 0, type
   = 1
LinkId =   2, out port =  57, rem port =  25, cost = 500, costCnt = 0, type
   = 1
LinkId =   2, out port =  60, rem port =   2, cost = 500, costCnt = 0, type
   = 1


--- <output truncated> ---
```

See Also

`interfaceshow`
`nbrstateshow`

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

ANEXO SWITCH TIPO 03
PARTE 3/B

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

memshow

Display the amount of free and used memory in switch.

Syntax `memshow [ -b | -k | -m ]`

Availability All users

Description Use this command to display free and used memory in the switch as well as the shared memory and buffers used by the kernel.

Operands This command has the following operands:

`-b`	Specify this operand to display memory usage in bytes. This is the default display value.
`-k`	Specify this operand to display memory usage in kilobytes.
`-m`	Specify this operand to display memory usage in megabytes.

By default the memory usage is displayed in bytes.

Example **To view the memory usage:**

```
switch:admin> memshow
              total        used        free      shared     buffers      cached
Mem:      129740800   112562176    17178624           0      139264    30396416
Swap:             0           0           0
switch:admin> memshow -m
              total        used        free      shared     buffers      cached
Mem:            123         107          16           0           0          28
Swap:             0           0           0
switch:admin>
```

See Also `savecore`

mscapabilityshow

Display the service support capability.

Syntax `mscapabilityshow`

Availability All users

Description Use this command to query a fabric for service support capability. This command provides information on what services are supported fabric wide.

The following capabilities are shown:

Bit 0: Basic Fabric Configuration Service Supported.
This bit displays the fabric capability to support Management Server. This service is available on all Brocade switches. This service is described in the FC-GS MS specification.

Bit 1: Platform Service Supported.
This bit displays the fabric capability to support the Management Server Platform Service. If the service is supported, you can enable it through the `msplmgmtactivate` command. This service is described in the FC-GS MS specification

Bit 2: Topology Discovery Service Supported.
This bit displays the fabric capability to support the Management Server Topology Discovery Service. If the service is supported, you can enable it through the `mstdenable "all"` command. This service is described in the FC-GS MS specification

Bit 3: Unzoned Name Service Supported.
This bit displays the fabric capability to support the Unzoned Name Server. This service is described in the FC-GS MS specification.

Bit 4: Fabric Zone Service Supported
This bit displays the fabric capability to support the Fabric Zone Service. This service is described in the FC-GS MS specification.

Bit 5: Fabric Lock Service Supported.
This service is not currently supported in Brocade switches, and defaults to 0. This service is described in the FC-GS MS specification.

Bit 6: Time Service Supported.
This bit displays the fabric capability to support the Time Service. For more information refer to the **tsclockserver** command. This service is described in the FC-GS MS specification.

Bit 7: RSCN Small Payload Supported.
This bit displays the fabric capability to support the RSCN Small Payload used by Name Server.

Bit 8: Reliable Commit Service (RCS) Supported.
The Reliable Commit Service (RCS) is an enhanced fabric wide commit service used by Security, Zoning, and Management Server.

To read the capabilities for a fabric, the hexadecimal value must be converted into binary. The binary value is read from right to left. A value of 1 means the switch is capable of supporting a given service, a value of 0 means the switch is not capable of supporting that service. For example, a capability value of `0x0000019f` would correspond to the following values:

Capability	8 7654 3210
Binary Value	1 1001 1111

In the above example, only Bit 5, Fabric Lock Service, and Bit 6, Time Service are not supported switch.

Operands None

Example To display Management Server capability on a fabric:

```
switch:admin> mscapabilityshow

      Switch WWN             Capability  Switch Name
=======================      ==========  ===========
10:00:00:60:69:90:03:f0      0x0000019f  "switch"*
10:00:00:60:69:90:24:f0      0x0000019f  "switch123"
10:00:00:60:69:90:31:f0      0x0000008f  "switch321"

        Capability Bit Definitions:
                Bit 0: Basic Fabric Configuration Service Supported.
                Bit 1: Platform Service Supported.
                Bit 2: Topology Discovery Service Supported.
                Bit 3: Unzoned Name Service Supported.
                Bit 4: Fabric Zone Service Supported.
                Bit 5: Fabric Lock Service Supported.
                Bit 6: Time Service Supported.
                Bit 7: RSCN Small Payload Supported.
                Bit 8: Reliable Commit Service(RCS) Supported.
                Others: Reserved.

Done.
switch:admin>
```

See Also
- msplmgmtactivate
- msplmgmtdeactivate
- msplatshow
- msplcleardb
- mstdenable
- mstddisable
- mstdreadconfig

msconfigure

Configure the Management Server.

Syntax msconfigure

Availability Admin

Description Use this command to display and configure parameters for Management Server. The Management Server enables a managment application to access and configure switches in the fabric. It is located at the fibre channel address, FFFFFAh.

If the Access Control List (ACL) is empty (default value), the Management Server is available to all systems connected in-band to

the fabric. To restrict access, specify the World Wide Name (WWN) for one or more management applications; access is then restricted to those WWNs. Up to 16 maximum WWNs are supported in the ACL.

The ACL is implemented on a per switch basis and should be configured on the switch to which the management application station is directly connected.

This command is interactive and provides the following choices:

0 Done

1 Display the access list

2 Add member based on its Port/Node WWN

3 Delete member based on its Port/Node WWN

If a change is made, you are prompted to save the changed ACL to non-volatile memory. The saved ACL is restored on future reboot.

When security is enabled, this command can run on any switch, but the ACL is only displayed from the Primary FCS.

Operands None

Example **To display the Management Server access control list.**

```
switch:admin> msconfigure

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 1

MS Access List consists of (5): {
20:01:00:60:69:00:60:10
20:02:00:60:69:00:60:10
20:03:00:60:69:00:60:10
20:02:00:60:69:00:60:03
20:02:00:60:69:00:60:15

0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 0

done ...
switch:admin>
```

See Also

```
mscapabilityshow
msplmgmtactivate
msplmgmtdeactivate
msplatshow
msplcleardb
mstddisable
mstdenable
mstdreadconfig
```

msplatshow

Display the Management Server Platform Database.

Syntax `msplatshow`

Availability All users

Description Use this command to display information from the Management Server Platform Database. The display shows the platform name and associated attributes of each object in the database.

Operands None

Example **To display the Management Server Platform Database for a fabric:**

```
switch:admin> msplatshow
---------------------------------------------------------
Platform Name: [9] "first obj"
Platform Type: 5 : GATEWAY
Number of Associated M.A.: 1
Associated Management Addresses:
[35] "http://java.sun.com/products/plugin"
Number of Associated Node Names: 1
Associated Node Names:
10:00:00:60:69:20:15:71
---------------------------------------------------------
Platform Name: [10] "second obj"
Platform Type: 7 : HOST_BUS_ADAPTER
Number of Associated M.A.: 1
Associated Management Addresses:
[30] "http://java.sun.com/products/1"
Number of Associated Node Names: 2
Associated Node Names:
10:00:00:60:69:20:15:79
10:00:00:60:69:20:15:75
```

See Also `mscapabilityshow`

msplmgmtactivate
msplmgmtdeactivate
msplcleardb

msplatshowdbcb

Display MS Platform Service Database Control Block.

Syntax msplatshowdbcb

Availability All users

Description Use this command to display the control block fields associated with the platform database.

Operands None

Example Display the MS Platform Service Database Control Block:

```
switch:admin> msplatshowdbcb
msPlDBCB.prevDList:
msPlDBCB.peerWwn == 00:00:00:00:00:00:00:00.
msPlDBCB.psPeerWwn == 00:00:00:00:00:00:00:00.
msPlDBCB.replicate == 0.
msPlDBCB.fabMaySeg == 255.
msPlDBCB.timeOutCnt == 0.
msPlDBCB.enabled == 0.
msPlDBCB.tid == (nil).
switch:admin>
```

See Also

mscapabilityshow
msconfigure
msplmgmtactivate
msplmgmtdeactivate
msplatshow
msplcleardb

msplcleardb

Clear the Management Server Platform Database on all switches in the fabric.

Syntax `msplcleardb`

Availability Admin

Description Use this command to clear the Management Server Platform Database on all switches in the fabric. Since this operation is non-recoverable (once issued, the database is erased), it should not be used unless it is intended to resolve a database conflict between two joining fabrics or to establish an entire new fabric with an empty database.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example To clear the Management Server Platform Database on all switches in the fabric:

```
switch:admin> msplcleardb
This will erase MS Platform Service Database in the entire fabric.

Would you like to continue this operation? (yes, y, no, n): [no] y

Request to MS Platform DB Clear operation in progress.....

*Fabric-wide MS Platform DB Clear operation in progress.....
switch:admin>
```

See Also `msplmgmtdeactivate`
`msplatshow`
`mscapabilityshow`
`msplmgmtactivate`

mspImgmtactivate

Activate the MS Platform Service on all switches in the fabric.

Syntax `msplmgmtactivate`

Availability Admin

Description Use this command to activate the MS Platform Service on all switches in the fabric. Run the `mscapabilityshow` command before issuing this command. If any switch within the fabric is not capable of running the MS Platform Service, the `msplmgmtactivate` command is rejected. When this command is issued, all the switches in the fabric will have the MS Platform Service enabled.

Once activated, even in the event of a reboot, the switch will initialize with the MS Platform Service enabled. By default, the MS Platform Service is disabled.

When security is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To activate MS Platform Service on all switches in the fabric:**

```
switch:admin> msplmgmtactivate

Request to activate MS Platform Service in progress......

*Completed activating MS Platform Service in the fabric!

switch:admin>
```

See Also

`msplmgmtdeactivate`
`msplatshow`
`mscapabilityshow`
`msplcleardb`

mspImgmtdeactivate

Deactivate the MS Platform Service on all switches in the fabric.

Syntax `mspImgmtdeactivate`

Availability Admin

Description Use this command to deactivate the MS Platform Service on all switches in the fabric. This command deactivates the MS Platform Service on each switch in the fabric and commits the changes to the non-volatile storage of each switch.

Once deactivated, even in the event of a reboot, the switch will initialize with the MS Platform Service disabled. By default, the MS Platform Service is disabled.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example **To deactivate the MS Platform Service on all switches in the fabric:**

```
switch:admin> msplmgmtdeactivate

MS Platform Service is currently enabled.

This will erase MS Platform Service configuration
information as well as database in the entire fabric.

Would you like to continue this operation? (yes, y, no, n): [no] y

Request to deactivate MS Platform Service in progress......

*Completed deactivating MS Platform Service in the fabric!
switch:admin>
```

See Also
- `msplatshow`
- `mscapabilityshow`
- `msplmgmtactivate`
- `msplcleardb`

mstddisable

Disable the Management Server Topology Discovery service.

Syntax `mstddisable [ALL]`

Availability Admin

Description Use this command to disable the Management Server Topology Discovery Service locally or fabric-wide. This command disables the Topology Discovery Service on the local switch and commits the changes to non-volatile memory of the local switch. If the operand ALL is used, then the command is executed on the entire fabric.

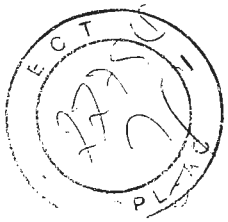
Once disabled, even in the event of a power cycle, the switch boots up with the Topology Discovery Service disabled.

The Topology Discovery Service requires that attached devices (including switches) support the RNID ELS command.

When security is enabled, and using the ALL operand, this command can only be issued from the Primary FCS switch.

Operands This command has the following operand:

ALL	Specify ALL to disable the Topology Discovery Service on all switches in the fabric. The operand ALL must be in capital letters. This operand is optional.



Example To disable the Management Server Topology Discovery service locally or fabric-wide:

```
switch:admin> mstddisable
This may erase all NID entries. Are you sure?  (yes, y, no, n): [no] y

Request to disable MS Topology Discovery Service in progress....
*MS Topology Discovery disabled locally.

switch:admin>
switch:admin> mstddisable ALL
This may erase all NID entries. Are you sure?  (yes, y, no, n): [no] y

Request to disable MS Topology Discovery Service in progress....
*MS Topology Discovery disabled locally.
*MS Topology Discovery Disable Operation Complete!!

switch:admin>
```

See Also `mstdenable`
`mstdreadconfig`

mstdenable

Enable the Management Server Topology Discovery service

Syntax `mstdenable [ALL]`

Availability Admin

Description Use this command to enable the Management Server Topology Discovery Service locally or fabric-wide. This command enables the Topology Discovery Service on the local switch and commits the changes to non-volatile memory of the local switch. If the operand `ALL` is used, then the command is executed on the entire fabric.

The Topology Discovery Service requires that attached devices (including switches) support the `RNID ELS` command.

When security is enabled, and using the `ALL` operand, this command can only be issued from the Primary FCS switch.

Operands This command has the following operand:

ALL	Specify ALL to enable the Topology Discovery Service on all switches in the fabric. The operand ALL must be in capital letters. This operand is optional.

Example **To enable the Management Server Topology Discovery Service locally or fabric-wide:**

```
switch:admin> mstdenable

Request to enable MS Topology Discovery Service in progress....
*MS Topology Discovery enabled locally.

switch:admin>
switch:admin> mstdenable ALL

Request to enable MS Topology Discovery Service in progress....
*MS Topology Discovery enabled locally.
*MS Topology Discovery Enable Operation Complete!!

switch:admin>
```

See Also mstddisable
mstdreadconfig

mstdreadconfig

Display the status of Management Server Topology Discovery service.

Syntax mstdreadconfig

Availability All users

Description Use this command to check whether or not the Management Server Topology Discovery service is enabled.

Operands None

Example **To display the status of the Topology Discovery service:**

```
switch:admin> mstdreadconfig

*MS Topology Discovery is enabled.

switch:admin>
```

See Also mstdenable

```
mstddisable
```

myid

Display the current login session details.

Syntax `myid`

Availability Admin

Description Use this command to display the status of the system and the login session details. The Status displays if the system is Redundant or Non-Redundant or Unknown.

The login session gives details of the following:

- Which CP/Switch (or console/serial port) was used to login
- The IP address of the current login session for telnet or the name of the current Console port or the Serial port (if modem login used).
- The Current CP's mode (Active or Standby or Unknown)
- The Current System Status (Redundant or Non-Redundant or Unknown).

Operands None

Example **To display current login information:**

```
switch:admin> myid
        Current Switch: switch
        Session Detail: switch (123.123.123.123) Active  Redundant
switch:admin>
```

See Also `version`

nbrstatsclear

Reset FSPF interface counters.

Syntax `nbrstatsclear [slotnumber/] [portnumber]`

Availability Admin

Description Use this command to reset the counters of FSPF frames transmitted and received on an interface.

Use this command with no operand to reset counters on all interfaces.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

When this command is specified with no operand, the statistics are cleared for all interfaces.

Examples **To display how to reset the counters on slot 1 port 4:**

```
switch:admin> nbrstatsclear 1/4
```

See Also

```
interfaceshow
portshow
switchshow
```

nbrstateshow

Display FSPF neighbor's state.

Syntax `nbrstateshow [slotnumber/] [portnumber]`

Availability All users

Description Use this command to display information about neighbors to the local switch, or information about a specific neighbor if a port number is supplied. A neighbor is a switch that is directly attached to the local switch. The display shows the following fields:

Local Domain IDDomain number of local switch.

Local Port	E_Port (interface) on local switch.
Domain	Domain number of remote switch.
Remote Port	E_Port (interface) on remote switch.
State	State of the neighbor. The E_Port is used to route frames only if the neighbor is in `NB_ST_FULL` state.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

Examples To display information about switches directly connected to the local switch:

```
switch:admin> nbrstateshow 1/3

Local Domain ID: 1

Local Port      Domain      Remote Port      State
------------------------------------------------------------
     3             4             0         NB_ST_FULL
switch:admin>
```

See Also interfaceshow

nodefind

Display all the device PIDs matching a given WWN.

Syntax nodefind "*WWN*"

Availability All users

Description Use this command to display the 24-bit Fibre Channel addresses of all the devices in the fabric that have either port world wide name or node world wide name matching with the given world wide name.

The message `No device is found with wwn xxxxxxxx` is displayed if there is no device matching the given *WWN*. If matches are found, the command displays the number of devices found.

Operands This command has the following operand:

WWN Specify the Worldwide Name which can be used to match the real device's port WWN or node WWN. The Worldwide Name must have eight colon separated fields each consisting of 1 or 2 hexadecimal digits between 0 and ff, with no spaces.

Example To display all the device PIDs matching a given WWN:

```
switch:admin> nodefind "50:05:07:65:05:04:08:e5"
1 device is found with wwn 50:05:07:65:05:04:08:e5
switch:admin>
```

See Also nsshow
nsallshow
nscamshow

nsaliasshow

Display local Name Server information with Aliases.

Syntax `nsaliasshow [-r]`

Availability All users

Description Use this command to display local name server information with the added feature of displaying the defined configuration aliases that the device belongs to.

The following message is displayed if there is no information in this switch:

```
There is no entry in the Local Name Server
```

There still may be devices connected to other switches in the Fabric. The command `nsallshow` shows information from all switches.

The display is identical to the command `nsshow` with the exception that an additional line is added for the aliases that the device belongs to after all other fields for the device. If there are no defined configuration aliases for that device, no alias is shown.

Options This command has the following option:

`-r`	Specify this option to replace the TTL attribute output with SCR (state change registration) information in the display. SCR is the state change registration of a device. This value indicates what type of RSCN a device registers to receive.

Example To display local Name Server information with Aliases:

```
switch:admin> nsaliasshow
Type Pid    COS     PortName                NodeName TTL(sec)
*N    011200;
2,3;10:00:00:60:69:00:ab:ba;10:00:00:60:69:00:ab:ba; 60
     FC4s: FCIP
     Fabric Port Name: 20:02:00:60:69:00:68:19
     Aliases:
NL   0214e4;
3;21:00:00:fa:ce:00:21:e1;20:00:00:fa:ce:00:21:e1; na
     FC4s: FCP [STOREX  RS2999FCPH3     CD09]
     Fabric Port Name: 20:04:00:60:69:01:44:22
     Aliases: MyAlias1 MyAlias2
N    021300;
3;10:00:00:60:69:00:02:d6;20:00:00:60:69:00:02:d6; na
     Fabric Port Name: 20:03:00:60:69:01:44:22
     Aliases: DeviceAlias

The Local Name Server has 3 entries
```

See Also `nsshow`
`nsallshow`
`switchshow`

nsallshow

Display global Name Server information.

Syntax `nsallshow [type]`

Availability All users

Description Use this command to display the 24-bit fibre channel addresses of all devices in all switches in the fabric. If the operand `type` is supplied, only devices of specified FC-PH type are displayed. If `type` is omitted, all devices are displayed.

Specifying the type operand causes the switch to send out a query to every switch in the fabric. On a large fabric it is recommended *not* to run a script that repeatedly issues the `nsallshow` command with a type operand specified.

Operands This command has the following operand:

type Specify the FC-PH type code. This operand is optional. The valid values for this operand are 0 to 255. Below are two specific FC-PH device type codes:

8 = FCP type device
4 , 5 = FC-IP type device

Other FC-PH types are displayed in the format "*x* ports supporting FC4 *code*" where *x* is the number of ports of a type, and *code* is the FC-PH type code.

Example **To display all devices in the Fabric, followed by all type 8 (SCSI-FCP) devices and all type 5 (SCSI-FCIP) devices:**

```
switch:admin> nsallshow
     12 Nx_Ports in the Fabric {
     011200 0118e2 0118e4 0118e8 0118ef 021200
     0214e2 0214e4 0214e8 0214ef
   }
switch:admin> nsallshow 8
     8 FCP Ports {
     0118e2 0118e4 0118e8 0118ef 0214e2 0214e4 0214e8 0214ef
      }
switch:admin> nsallshow 5
    2 FC-IP Ports in the Fabric {
    011200 021200}
```

See Also `nsshow`
`switchshow`

nscamshow

Display information about remote devices in the Name Server Cache.

Syntax `nscamshow`

Availability All users

Description Use this command to display the local Name Server Cache information about the devices discovered in the fabric by the Name Server Cache manager.

The message `No Entry found!` is displayed if the Name Server Cache Manager hasn't discovered new switches and any new devices in the fabric.

For each remote switch found the output of this command shows the domain number, state, revision, owner, the list of cold and hot devices for that domain number. For each device found in the cold or hot devices list, the following information is displayed:

Type	U for unknown, N for N_Port, NL for NL_Port.
Pid	The 24-bit Fibre Channel address.
COS	A list of classes of service supported by the device.
PortName	The device's port Worldwide Name.
NodeName	The device's node Worldwide Name.

There may be additional lines if the device has registered any of the following information (the switch automatically registers SCSI inquiry data for FCP target devices): FC4s supported and fabric port name.

Operands None

Example **To displays all Switch and device entries discovered by the Name Server in the fabric.:**

```
switch:admin> nscamshow

nscam show for remote switches:

Switch entry for 2
state   rev     owner
cold    v250+   0xfffc01

Hot device list:
No Entry found!

Cold device list:
Type Pid    COS     PortName                NodeName
N    021200;    2,3;10:00:00:60:69:00:ab:ba;10:00:00:60:69:00:ab:ba;
FC4s: FCIP      Fabric Port Name: 20:02:00:60:69:00:68:19
```

See Also nsshow
nsallshow
switchshow

nsshow

Display local Name Server information.

Syntax `nsshow [-r]`

Availability All users

Description Use this command to display local Name Server information, including information about devices connected to this switch, and cached information about devices connected to other switches in the fabric.

The following message is displayed if there is no information in this switch:

```
There is no entry in the Local Name Server
```

There still may be devices connected to other switches in the fabric. The command `nsallshow` displays information from all switches. Each line of output shows:

*	Indicates a cached entry from another switch.
Type	U for unknown, N for N_Port, NL for NL_Port.
PID	24-bit fibre channel address.
COS	List of classes of service supported by device.
PortName	Device port Worldwide Name.
NodeName	Device node Worldwide Name.
TTL	Time-to-live (in seconds) for cached entries, or NA (not applicable) if the entry is local.
SCR	State change registration of the device. This is displayed if `-r` option is given.

There may be additional lines if the device has registered any of the following information (the switch automatically registers SCSI inquiry data for FCP target devices):

- FC4s supported
- IP address
- IPA
- Port and node symbolic names

- Fabric Port Name - This is the WWN of the port on the switch that the device is physically connected to.
- Hard address and/or port IP address

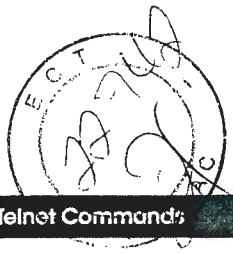
Options This command has the following option:

`-r` Specify this option to replace the TTL attribute output with SCR (state change registration) information in the display. SCR is the state change registration of a device. This value indicates what type of RSCN a device registers to receive.

Example **To display local name server information:**

```
switch:admin> nsshow -r
{
 Type Pid    COS     PortName                NodeName                SCR
 NL   2016ce;      3;21:00:00:04:cf:75:78:d2;20:00:00:04:cf:75:78:d2; 0
    FC4s: FCP [SEAGATE ST318452FC      0001]
    Fabric Port Name: 20:16:00:60:69:90:03:f8

 N    201700;      3;21:00:00:e0:8b:05:a3:c9;20:00:00:e0:8b:05:a3:c9; 1
    Fabric Port Name: 20:17:00:60:69:90:03:f8

The Local Name Server has 2 entries }
switch:admin>
```

See Also `nsallshow`
`switchshow`



nsstatshow

Display local Name Server statistical information

Syntax nsstatshow

Availability All users

Description Use this command to display local Name Server statistic information.

Operands None

Example **To display local Name Server statistical information:**

```
switch:admin> nsstatshow
Name Server Statistics {
          69 invoked                2 invokedErr              0 noBuf
  Input
           0 discards               0 errors                  3 accepted
           0 rejected
  Output
           0 request                0 errors                  0 unexpected
           0 cached                 0 timedout                0 truncated
  Req. breakdown
           0 G?_ID                  0 G?_NN                   0 GID_NN
           1 GID_FT                 4 GID_PT                  0 GID_FF
           0 GPN_FT                 0 GNN_FT                  0 GA_NXT
           1 R?_ID                  0 R?_NN                   0 other
}
Name Server to Server Communication Statistics {
  Input
           0 requests              48 accepts                4 rejects
           0 informs                0 deletions
           2 ge_id                  0 ge_pn                   0 ge_nn
  Output
          52 requests              52 accepts                15 rejects
           0 informs                0 deletions               0 truncations
  Errors
           0 nobuf                  0 inErrors                0 inDiscards
           0 outErrors              0 unexpected
}

switch:admin>
```

See Also nsallshow
nsshow
nscamshow
switchshow

nszonemember

Display the information of all the online devices which are zoned with the given device.

Syntax `nszonemember` *`OxPID`*

Availability All users

Description Use this command to display the information of all the online devices which are zoned with the given device. Each line of output shows:

Type	U for unknown, N for N_Port, NL for NL_Port.
Pid	The 24-bit Fibre Channel address.
COS	A list of classes of service supported by the device.
PortName	The device's port Worldwide Name.
NodeName	The device's node Worldwide Name.

There may be additional lines if the device has registered any of the following information (the switch automatically registers SCSI inquiry data fro FCP target devices):

- FC4 supported
- IP address (node)
- IPA
- port and node symbolic name (local device only)
- fabric port name
- hard address and/or port IP address.

Operands This command has the following operand:

`OxPID`	Specify the port ID whose zoned devices are to be viewed. This operand is required.

Example To display the information of all the online devices which are zoned with the given device:

```
switch:admin> nszonemember 0x0416e2
3 local zoned members:

Type Pid    COS     PortName                NodeName                 T
NL   041901;    2,3;10:00:00:00:c9:26:0e:ae;20:00:00:00:c9:26:0e:ae; n
Fabric Port Name: 20:09:00:60:69:50:06:78
NL   0416e2;      3;22:00:00:20:37:d9:6b:b3;20:00:00:20:37:d9:6b:b3; n
FC4s: FCP [SEAGATE ST318304FC      0005]
Fabric Port Name: 20:06:00:60:69:50:06:78
NL   0416e4;      3;22:00:00:20:37:d9:61:ac;20:00:00:20:37:d9:61:ac; n
FC4s: FCP [SEAGATE ST318304FC      0005]
Fabric Port Name: 20:06:00:60:69:50:06:78

No remote zoned members
```

See Also nsshow
nscamshow
cfgshow

passwd

Change the password for a user level.

Syntax `passwd ["user"]`

Availability All users

Description Use this command to change the password for the user currently logged in, or, for another user. To change the password for a specific user, enter the command with the optional *user* operand.

The hierarchy of user levels are (from greatest access to least) is root, factory, admin, and user. Typically, all fabric management should be performed from the admin user.

When the root password is changed, all user levels currently logged in are terminated.

If the fabric is not in secure mode, the behavior of the command is as follows:

- If you are changing your own user level password, you are prompted to enter the old password, and if it is valid, then the new password.

- If a you are changing another user level password, you are prompted to enter that user level's old password, and if it is valid, then the new password.
- If you are logged in as the root user when changing another user level password, you are not prompted to enter the old password.
- The command is disabled until you have changed all the login passwords from the manufacture default values.

If the fabric is in secure mode, the behavior of the command is as follows:

- If you change your current login level password, you are also prompted to change the passwords of all the user levels below your current level in the user level hierarchy. For example, if you execute this command as the admin user, you are prompted to change the password of the user account, as user is below admin in the hierarchy. If you execute this command as the root level, then you are prompted to change the passwords of factory, admin, and user. If the command is aborted at any point, the current passwords are not changed for any user level.
- The command can only be run on the primary FCS switch. The changed passwords will be distributed to all FCS switches. Non-FCS switches will be updated if the password of the user account is changed.
- Changing the password of any user level will cause the login session of that account (if logged in) to be terminated.

If the Security option is enabled on the fabric this command is disabled on all switches except the Primary FCS. Refer to the *Secure Fabric OS User's Guide* for more information.

A new password must fulfill these rules,

- must have 8 to 40 characters,
- must not be the same as the previous password.

Use the following to control input:

RETURN — When entered at a prompt with no preceding input, accepts the default value (if applicable) and moves to the next prompt.

CONTROL-D (end of file)
When entered at a prompt with no preceding input, it terminates the command without changing password. This is valid on most computers, however, your settings could be different.

Operands

This command has the following operands:

user — Specify the name of the user, in quotation marks, where you want to modify the password. This operand is optional. Valid values are: root, factory, admin, or user. You can only specify this operand when you are logged in as root, factory, or admin. If you try to change the password of a user level who is higher in hierarchy (for example admin changing the root password), you are prompted to enter the current password of that level. If you try to change the password of a user level who is lower in hierarchy, you are not prompted to enter the current password.

Example

To change the password for the admin user:

```
switch:admin> passwd "admin"
Changing password for admin
Enter new password:
Re-type new password:
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.
switch:admin>
```

Errors

When failures are detected, the subtext may report one or more of the following error messages:

"user" is not a valid user name.	You have not specified a user name that is a valid, recognized user name on the system.
Permission denied.	You do not have permission to change the login name or password specified.
Incorrect password.	You have not entered the correct password when prompted for the old password.
Password unchanged.	You have entered the carriage return special input case, choosing not to change the password.
Passwords do not match.	You have not correctly verified the new password.

See Also

`login`
`logout`

pdshow

Display data from a panic dump file.

Syntax

`pdshow [panic-dump-file]`

Availability

Admin

Description

Use this command to display data from a panic dump file. The panic dump file contains information that may be useful to determine the cause of the system panic.

When executed without any arguments, this command displays output from the latest panic dump file available on the switch.

If a panic dump file is specified as an argument, the contents of that specific file are displayed.

Operands

This command has the following operands:

panic-dump-file	Specify the full path name of a panic dump file. This operand is optional.

Example The following example shows how `pdshow` can be used to examine a panic dump file by the name `panic_dump` located under the directory `/tmp`.

```
switch:admin> pdshow /tmp/panic_dump

                *** CAUTION ***
  *  Host  PLATFORM  (current) is: 'Unknown'
  *  PLATFORM got from pd file is: 'SW12000'
  *  Some restuls shown may be incorrect and/or missing
  *  It is best if this command is run on same PLATFORM as that of pdfile
              **************

                        ********
*   File   :/core_files/panic/core.pd1038932352       *
*   SECTION:PD_MISC                                   *
-----------------------********-------------------------
WatchDogRegister=0x0
Section=Startup time: Tue Dec  3 16:06:11 UTC 2002
Kernel=     2.4.19
Fabric OS=  v4.1.0_j_dist_1103
Made on=    Tue Dec 3 19:07:13 2002
Flash=      Tue Dec 3 13:19:06 2002
BootProm=   3.2.0
Section=HA show Output

--- <output truncated> ---
```

See Also `savecore`
`portlogdump`

perfaddeemonitor

Add end-to-end monitor to a port.

Syntax

```
perfaddeemonitor [slotnumber/]portnumber "SourceID"
"DestID"
```

Availability

Admin

This command requires a Performance Monitor license.

Description

Use this command to add an End-to-End performance monitor to a port. Only frames transmitted are counted. The performance monitor counts the number of words received, number of words transmitted and number of CRC errors detected using either of the following two conditions:

- for frames received at the port the frame SID is the same as `SourceID` and frame DID is the same as `DestID`. Both RX_COUNT and CRC_COUNT will be updated accordingly. Note that the CRC_COUNT will count the CRC errors detected with the frames received at or transmitted from the associated port.
- for frames transmitted from the port the frame DID is the same as `SourceID` and frame SID is the same as `DestID`, both TX_COUNT and CRC_COUNT will be updated accordingly.

Depending on the application, any port along the routing path can be selected for such monitoring.

For example, to monitor traffic flowing from point A, receiving at port C and transmitting at port D to reach point B, and the traffic flowing back from B to A. You can install a monitor on port C, specify point A as `SourceID` and point B as `DestID`. Then RX_COUNT counts the traffic flow from A to B, CRC_COUNT counts the frames with CRC errors from both directions. TX_COUNT counts the traffic from B to A.

Similarly, you can install a monitor on port D, specify point B as `SourceID` and point A as `DestID`. Then RX_COUNT counts the traffic from B to A, CRC_COUNT counts the frames with CRC errors from both directions and TX_COUNT counts the traffic from A to B.

End-to-End monitors traffic on the receiving port, respective to the `SourceID`.

RX_COUNT are associated with frames received at the port. CRC_COUNT is associated with frames received at and transmitted from the port. TX_COUNT is associated with frames transmitted from the port.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these performance monitors.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
SourceID	Specify the 3-byte SID (Source ID) of the originator device. It should be in "0xDDAAPP" format, where DD is Domain ID, AA is Area ID and PP is ALPA ID. For example, `0x058e0f`, has a Domain ID of "5", an Area ID of "8e" and an ALPA ID of "f".
DestID	Specify the 3-byte DID (Destination ID) of the destination device. It should be in "0xDDAAPP" format, where DD is Domain ID, AA is Area ID and PP is ALPA ID. For example, `0x058e0f`, has a Domain ID of "5", an Area ID of "8e" and an ALPA ID of "f".

Example **To add an end-to-end monitor to blade 1 port 2:**

```
switch:admin> perfaddeemonitor 1/2 "0x058e0f" "0x1182ef"
End-to-End monitor number 0 added.
switch:admin>
```

See Also

```
perfaddipmonitor
perfaddreadmonitor
perfaddrwmonitor
perfaddscsimonitor
perfaddusermonitor
perfaddwritemonitor
```

perfaddipmonitor

Add a filter-based monitor for IP frame count.

Syntax `perfaddipmonitor [slotnumber/]portnumber ["alias"]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to define filter-based monitors to count the number of IP traffic frames. Only frames transmitted are counted.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these filter-based performance monitors. The optional user defined alias is also displayed if one was specified. All valid monitor numbers and user-defined aliases can be displayed with the `perfshowfiltermonitor` command.

There is no need to define multiple IP frame monitors on a port.

Operands This command has the following operands:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

alias Specify a name for this monitor. This character string can be a maximum of 10 characters long and must be enclosed in quotation marks. This operand is optional. The default alias is IP FRAME.

Example

To add an IP monitor to a port:

```
switch:admin> perfaddipmonitor 1/4 "IP_MONITOR"
IP traffic frame monitor #0 added
switch:admin>
```

See Also

```
perfaddeemonitor
perfaddreadmonitor
perfaddrwmonitor
perfaddscsimonitor
perfaddusermonitor
perfaddwritemonitor
```

perfaddreadmonitor

Add a filter-based monitor for the SCSI Read command

Syntax `perfaddreadmonitor [slotnumber/]portnumber ["alias"]`

Availability Admin

This command requires a Performance Monitor license

Description Use this command to define filter-based monitors to count the number of SCSI FCP Read commands in Fibre Channel frames. Only frames transmitted are counted.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these filter-based performance monitors. The optional user defined alias is also displayed if one was specified. All valid monitor numbers and user-defined aliases can be retrieved with the `perfshowfiltermonitor` command. The maximum number of filters is 8 per port including user-defined filters, read filters, write filters, read/write filters, SCSI frame monitor, and IP frame monitor.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

alias Specify a name for this monitor. The character string can be a maximum of 10 characters long and is truncated if more characters are specified. This operand must be enclosed in quotation marks. This operand is optional. The default alias is SCSI Read.

Example

To add a SCSI Read monitor to a port:

```
switch:admin> perfaddreadmonitor 2/4 "SCSI_R"
SCSI Read filter monitor #2 added
switch:admin>
```

See Also

```
perfaddeemonitor
perfaddipmonitor
perfaddrwmonitor
perfaddscsimonitor
perfaddusermonitor
perfaddwritemonitor
```

perfaddrwmonitor

Add a monitor for the SCSI read and write commands.

Syntax `perfaddrwmonitor [slotnumber/]portnumber ["alias"]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to define filter-based monitors to count the number of SCSI FCP Read and Write commands in Fibre Channel frames. Only frames transmitted are counted.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these filter-based performance monitors. The optional user defined alias is also displayed if one was specified. All valid monitor numbers and user-defined aliases can be retrieved with the `perfshowfiltermonitor` command.

The maximum number of filters is 8 per port including user-defined filters, read filters, write filters, read/write filters, SCSI frame monitor, and IP frame monitor.

Operands This command has the following operands:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

`portnumber` Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

alias	Specify a name for this monitor. This character string can be a maximum of 10 characters long and is truncated if more characters are specified. This operand must be enclosed in quotation marks. This operand is optional. The default alias is SCSI R/W.

Example **To add a SCSI read and write monitor to a port:**

```
switch:admin> perfaddrwmonitor 2/4 "SCSI_RW"
SCSI Read/Write monitor #1 is added
switch:admin>
```

See Also

```
perfaddeemonitor
perfaddipmonitor
perfaddreadmonitor
perfaddscsimonitor
perfaddusermonitor
perfaddwritemonitor
```

perfaddscsimonitor

Add a monitor for SCSI frame count.

Syntax `perfaddscsimonitor [slotnumber/]portnumber ["alias"]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to define filter-based monitors to count the number of SCSI traffic frames. Only frames transmitted are counted.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these filter-based performance monitors. The optional user defined alias is also displayed if one was specified. All valid monitor numbers and user-defined aliases can be retrieved with the `perfshowfiltermonitor` command.

There is no need to define multiple SCSI frame counters on a port.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
alias	Specify a name for this monitor. This character string can be a maximum of 10 characters long and is truncated if more characters are specified. This operand must be enclosed in quotation marks. This operand is optional. The default alias is SCSI Frame.

Example **To add a SCSI traffic frame monitor to a port:**

```
switch:admin> perfaddscsimonitor 2/4 "SCSI_FR"
SCSI traffic frame monitor #0 added
switch:admin>
```

See Also

```
perfaddeemonitor
perfaddipmonitor
perfaddreadmonitor
perfaddrwmonitor
perfadduermonitor
perfaddwritemonitor
```

perfaddusermonitor

Add a user-defined filter-based monitor.

Syntax `perfaddusermonitor [slotnumber/]portnumber "grouplist" ["alias"]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to define a special mechanism to qualify frames for statistics gathering to fit your own special need. Only frames transmitted are counted.

Each group of elements with same offset will have their comparison result (OR-ed) together before the combined result of each group gets (AND-ed) together for final comparison result. If the final result is logic 1, then the monitor counter will be increased by one.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these filter-based performance monitors. The optional user-defined alias is also displayed if one was specified. All valid monitor numbers and user-defined aliases can be retrieved with the `perfshowfiltermonitor` command.

The maximum number of filters is 8 per port including user defined filters, read filters, write filters, read/write filters, SCSI frame monitor, and IP frame monitor. In addition there should be no more than 6 different Offsets for each filter and no more than 4 different values per Offset defined by user. Though you can only configure 6 unique offsets per port, multiple filters can have the same 6 offsets.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number

5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

grouplist Specify up to 6 sets of Offset, Mask, and ValueList separated by a semicolon (;). The entire grouplist operand must be enclosed in quotation marks. This operand is required.

The grouplist operand must be specified in the following format:

```
"offset, Mask, ValueList; offset, Mask, ValueList"
```

For example:

```
"4, 0xff, 0x22; 12, 0xff, 0x01"
```

The `grouplist` component values are as follows:

`Offset` - Specify the offset within the frame. Offset `0` is the first byte of the SOF, and offset `4` is the first byte of the frame header. The Offset must be in decimal format. Valid values for Offset are `0`, [`4-63`]. Offset `0` is a special case which can be used to monitor the first 4 bytes SOFx frames. EOF can not be monitored.

`Mask` - Specify the mask value to be applied (ANDed) to frame contents.

`ValueList` - Specify up to four values that need to be captured from frame contents. The `ValueList` can be either hexidecimal or decimal format.

SOFx frames are considered a special case. The Offset is specified as 0x0, `valueList` are specified with:

`0` - SOFf

`1` - SOFc1

`2` - SOFi1

`3` - SOFn1

4 - SOFi2

5 - SOFn2

6 - SOFi3

7 - SOFn3

alias Specify a name for this monitor. This character string can be a maximum of 10 characters long and is truncated if more characters are specified. This operand must be enclosed in quotation marks. This operand is optional.

Example **To add a filter based monitor for all Extended Link Service request (R_CTL=0x22 and TYPE=0x01) to a port:**

```
switch:admin> perfaddusermonitor 1/4 "4, 0xff, 0x22; 12, 0xff, 0x01"
User monitor #0 added
switch:admin>
```

As a special case, to add a filter based monitor for SOFI3 to a port:

```
switch:admin> perfaddusermonitor 1/4 "0, 0xff, 6"
User monitor #1 added
switch:admin>
```

See Also

```
perfaddeemonitor
perfaddipmonitor
perfaddreadmonitor
perfaddrwmonitor
perfaddscsimonitor
perfaddwritemonitor
```

perfaddwritemonitor

Add a filter-based monitor for the SCSI Write command.

Syntax `perfaddwritemonitor [slotnumber/]portnumber "alias"]`

Availability Admin

This command requires a Performance Monitor license.

Description

Use this command to define filter-based monitors to count the number of SCSI FCP Write commands in Fibre Channel frames. Only frames transmitted are counted.

After a successful execution of this command, a monitor number is displayed. The monitor number is provided for easy manipulation of these filter-based performance monitors. The optional user- defined alias is also displayed if one was specified. All valid monitor numbers and user-defined aliases can be retrieved with the `perfshowfiltermonitor` command. The maximum number of filters is 8 per port including user-defined filters, read filters, write filters, read/write filters, SCSI frame monitor, and IP frame monitor.

Operands

This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
alias	Specify a name for this monitor. This character string can be a maximum of 10 characters long and is truncated if more characters are specified. This operand must be enclosed in quotation marks. This operand is optional. The default alias is SCSI_Write.

Example

To add a SCSI Write command monitor to a port:

```
switch:admin> perfaddwritemonitor 2/4 "SCSI_W"
SCSI Write filter monitor #0 added
switch:admin>
```

See Also

```
perfaddeemonitor
perfaddipmonitor
perfaddreadmonitor
```

perfaddrwmonitor
perfaddscsimonitor
perfaddusermonitor

perfcfgclear

Clear the previously saved performance monitoring configuration settings from non-volatile memory.

Syntax perfcfgclear

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to clear the previously saved end-to-end and filter configuration settings of performance monitoring from non-volatile memory.

Operands None

Example **To clear the performance monitoring information from non-volatile memory:**

```
switch:admin> perfcfgclear
This will clear Performance Monitoring settings in FLASH ROM.
The RAM settings won't change. Do you want to continue? (yes, y, no, n):
   [no] y
Please wait ...
Performance Monitoring configuration cleared from FLASH.
switch:admin>
```

See Also perfcfgrestore
perfcfgsave

perfcfgrestore

Restore performance monitoring configuration settings from non-volatile memory.

Syntax `perfcfgrestore`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to restore the performance monitoring configuration information from non-volatile memory. This does not restore the information cleared using the `perfcfgclear` command, rather it restores the configuration on non-volatile memory. Any configuration changes that were not saved are lost using the `perfcfgclear` command.

Operands None

Example **To restore the performance monitoring configuration information from non-volatile memory:**

```
switch:admin> perfcfgrestore
This will overwrite current Performance Monitoring settings
in RAM. Do you want to continue? (yes, y, no, n): [no] y
Please wait ...
Performance monitoring configuration restored from FLASH ROM.
switch:admin>
```

See Also `perfcfgclear`
`perfcfgsave`

perfcfgsave

Save performance monitoring configuration settings to non-volatile memory.

Syntax `perfcfgsave`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to save the current end-to-end and filter configuration settings of performance monitoring into non-volatile memory. This enables the performance monitoring configuration to be saved over power off cycles.

Operands None

Example **To save the current performance monitoring configuration to firmware:**

```
switch:admin> perfcfgsave
This will overwrite previously saved Performance Monitoring
settings in FLASH ROM. Do you want to continue? (yes, y, no, n): [no] y
Please wait ...
Performance monitoring configuration saved in FLASH ROM.
switch:admin>
```

See Also `perfcfgclear`
`perfcfgrestore`

perfcleareemonitor

Clears statistics counters of an end-to-end monitor on a port.

Syntax `perfcleareemonitor [slotnumber/]portnumber [monitorId]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to clear statistics counters for all or a specified end-to-end monitor on a port.

After a successful execution of this command, a message displays confirming that this monitor's counters have successfully been cleared. Prior to issuing this command, verify all the valid end-to-end monitor numbers on a specific port using the `perfshoweemonitor` command to make sure that the right monitor's counters will be cleared.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

monitorId Specify the monitor number you want to clear. Monitor numbers are defined when you create the monitor on a port. This operand is optional. If not specified, all monitors's counters on the port will be cleared.

Example To clear statistics counters for an end-to-end monitor:

```
switch:admin> perfcleareemonitor 1/2 5
End-to-End monitor number 5 counters are cleared
switch:admin>
switch:admin> perfcleareemonitor 1/2
This will clear ALL EE monitors' counters on port 2, continue? (yes, y, no,
   n):
[no] y
switch:admin>
```

See Also `perfshoweemonitor`
`perfaddeemonitor`

perfclearfiltermonitor

Clears statistics counters of a filter-based monitor.

Syntax `perfclearfiltermonitor [`*`slotnumber/`*`]`*`portnumber`*
`[`*`monitorId`*`]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to clear statistics counters for all or a specified filter-based monitor.

After a successful execution of this command, a message displays confirming that this monitor's counters have successfully been cleared. Prior to issuing this command, verify all the valid monitor numbers user-defined aliases on a specific port using the `pershowfiltermonitor` command to make sure that the right monitor's counters are cleared.

Operands This command has the following operands:

`slotnumber`	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

monitorId Specify the monitor number you want to clear. Monitor numbers are defined when you create the monitor on a port. This operand is optional. If not specified, all monitors's counters on the port will be cleared.

Example **To clear statistics counters for a filter-based monitor:**

```
switch:admin> perfclearfiltermonitor 1/2 4
Filter-based monitor number 4 counters are cleared
switch:admin>
switch:admin> perfclearfiltermonitor 1/2
This will clear ALL filter-based monitors' counters on port 2, continue?
   (yes, y
, no, n): [no] y
switch:admin>
```

See Also `perfshowfiltermonitor`
`perfaddusermonitor`

perfclralpacrc

Clear an ALPA device's CRC count by the port and ALPA.

Syntax `perfclralpacrc [slotnumber/]portnumber [ALPA]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to clear a specific ALPA device's CRC error counter. If the ALPA is provided as an operand only the counters for that device are reset; if no ALPA is specified this command clears the CRC counters for all ALPA devices on the specified port.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

ALPA Specify the ALPA address if you want to clear the CRC error counter for a particular device. This operand is optional.

Example **To clear CRC count on a particular ALPA on a port, and then clear CRC count for all ALPAs on a port:**

```
switch:admin> perfclralpacrc 2/15 0x59
CRC error count at ALPA 0x59 on port 31 is cleared.
switch:admin>
switch:admin> perfclralpacrc 2/15
This will clear all ALPA CRC Counts on port 31
Do you want to continue? (yes, y, no, n)y
Please wait ...
All alpa CRC counts are cleared on port 31.
switch:admin>
```

See Also `perfshowalpacrc`

perfdeleemonitor

Delete an end-to-end monitor from a port.

Syntax `perfdeleemonitor [slotnumber/]portnumber [monitorId]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to delete an end-to-end monitor from a port.

After a successful execution of this command, a message displays confirming that this monitor has successfully been deleted. Prior to issuing this command, verify all the valid end-to-end monitor numbers on a specific port using the **perfshowfiltermonitor** command to make sure that the right monitor is deleted.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
monitorId	Specify the monitor number you want to delete. Monitor numbers are defined when you create the monitor on a port. This operand is optional. When not specified, all monitors on the port are deleted.

Example To delete an end-to-end monitor on a port:

```
switch:admin> perfdeleemonitor 7/2 5
End-to-End monitor number 5 deleted
switch:admin>
switch:admin> perfdeleemonitor 7/2
This will remove ALL EE monitors on port 2, continue? (yes, y, no, n): [no]
   y
switch:admin>
```

See Also `perfshoweemonitor`
`perfaddeemonitor`

perfdelfiltermonitor

Delete a filter-based monitor from a port.

Syntax `perfdelfiltermonitor [slotnumber/]portnumber [monitorid]`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to delete a filter-based monitor from a port.

After a successful execution of this command, a message displays confirming that this monitor has successfully been deleted. Prior to issuing this command, verify all the valid monitor numbers and user-defined aliases on a specific port using the `perfshowfiltermonitor` command to make sure that the right monitor is deleted.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number

5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

monitorid Specify the monitor number you want to delete. Monitor numbers are defined when you create the monitor on a port. This operand is optional. If no operand is specified, all monitors on the port are deleted.

Example **To delete filter monitor 4 from a port:**

```
switch:admin> perfdelfiltermonitor 2/3 4
The specified filter-based monitor is deleted.
switch:admin> perfdelfiltermonitor 2/3
This will remove ALL monitors on port 19, continue? (yes, y, no, n): [no] y
switch:admin>
```

See Also `perfshowfiltermonitor`
`perfaddusermonitor`

perfhelp

Display performance monitoring help information.

Syntax `perfhelp`

Availability All users

This command requires a Performance Monitor license.

Description Use this command to display the available performance monitoring help commands.

Operands None

Example To display commands related to performance monitoring:

```
switch:admin> perfhelp

perfCfgSave                    Save Performance configuration to FLASH
perfCfgRestore                 Restore Performance configuration from FLASH
perfCfgClear                   Clear Performance settings from FLASH
perfClrAlpaCrc                 Clear ALPA device's CRC count
perfShowAlpaCrc                Get ALPA CRC count by port and ALPA
perfAddEEMonitor               Add end-to-end monitor to a port
perfDelEEMonitor               Delete an end-to-end monitor on port
perfClearEEMonitor             Clear an end-to-end monitors' counters on a
   port
perfShowEEMonitor              Show user-defined end-to-end monitors
perfSetPortEEMask              Set overall mask for E-to-E monitors
perfShowPortEEMask             Show the current end-to-end mask
perfAddUserMonitor             Add filter-based monitor
perfAddReadMonitor             Add filter-based monitor - SCSI Read
perfAddWriteMonitor            Add filter-based monitor - SCSI Write
perfAddRWMonitor               Add monitor - SCSI Read and Write
perfAddSCSIMonitor             Add monitor for SCSI frame count
perfAddIPMonitor               Add monitor for IP trafic frame count
perfDelFilterMonitor           Delete filter-based monitor
perfClearFilterMonitor         Clear filter-based monitors' counters on a
   port
perfShowFilterMonitor          Show filter-based monitors

switch:admin>
```

perfsetporteemask

Set overall mask for end-to-end (EE) monitors.

Syntax `perfsetporteemask [slotnumber/]portnumber "TxSIDMsk" "TxDIDMsk" "RxSIDMsk" "RxDIDMsk"`

Availability Admin

This command requires a Performance Monitor license.

Description Use this command to set the mask for the EE monitors of a port. This command enables a user to selectively choose the kind of fibre channel frames in which the number of words are to be counted.

This command enables you to identify one or all of the address fields (Domain ID, Aread ID, Alpa ID) of the SID or DID to trigger the monitor.

When a mask is set (0xff), the corresponding field will be used to trigger the monitor. If the mask is unset (0x00), the corresponding field will be ignored.

There is only one EE mask per port. The mask is applied to all eight EE monitors available on a port. The default EE mask value upon power-on is all set. When you change the mask, the counters are also reset to 0.

Operands

This command has the following operands:

slotnumber — Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber — Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

TxSIDMsk — Specify the source ID mask in `dd:aa:pp` format, where `dd` is Domain ID mask, `aa` is Area ID mask and `pp` is ALPA ID mask. For example, `00:ff:00` uses TxSID Area ID to trigger the EE monitor. *TxSIDMsk* stands for Transmitting Source ID Mask.

Specify the following values to turn on or off a specific field:
00 - Specifies that the field does not trigger EE monitors.
ff - Specifies that the field does triggers EE monitors.
This operand must be enclosed in quotation marks. This operand is required.

TxDIDMsk — Specify the destination ID mask in `dd:aa:pp` format. This operand must be enclosed in quotation marks. *TxDIDMsk* stands for Transmitting Destination ID Mask. This operand is required.

RxSIDMsk Specify the source ID mask in `dd:aa:pp` format. This operand must be enclosed in quotation marks. *RxSIDMsk* stands for Receiving Source ID Mask. This operand is required.

RxDIDMsk Specify the destination ID mask in `dd:aa:pp` format. This operand must be enclosed in quotation marks. *RxDIDMsk* stands for Receiving Destination ID Mask. This operand is required.

Example **To set the overall mask for end-to-end monitors on a port:**

```
switch:admin> perfsetporteemask 1/6 "00:00:00" "ff:ff:ff" "00:00:ff"
   "ff:00:00"
The EE mask on port 6 is set and EE counters are reset.
switch:admin>
```

See Also `perfaddeemonitor`

perfshowalpacrc

Display the ALPA CRC count by port or by ALPA.

Syntax `perfshowalpacrc [slotnumber/]portnumber [ALPA]`

Availability All users

This command requires a Performance Monitor license.

Description Use this command to display a specific ALPA device CRC error count by the port or ALPA. If the ALPA operand is specified, only the CRC count for that ALPA device is displayed. If the ALPA operand is not specified, the CRC count for all the ALPA devices on a specified port are displayed. CRC count is a 64-bits counter. When the count is over 32 bits, the CRC count value is displayed in hexidecimal. Otherwise, CRC count is displayed in decimal format.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port

number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

ALPA Specify the ALPA address if you want to get the CRC errors for a particular device. This operand is optional.

Example **To display the CRC error count for all ALPA devices on a port:**

```
switch:admin> perfshowalpacrc 2/4
ALPA                CRC_ERROR_COUNT
-----------------------------------
0x01                0
switch:admin>
```

See Also `perfclralpacrc`

perfshoweemonitor

Display end-to-end monitor information and frame traffic on a port.

Syntax **perfshoweemonitor** `[`*slotnumber*`/]`*portnumber* `[`*interval*`]`

Availability All users

This command requires a Performance Monitor license.

Description Use this command to display end-to-end monitor information and frame traffic on a port. This command can display (if no interval operand is specified):

- Key - the monitor number
- SID - Sending ID
- DID - Destination ID
- Owner_app - TELNET or WEB_TOOLS

- Owner_ip_addr - the IP address of the filter monitor owner
- Tx_count - Number of FC words transmitted
- Rx_count - Number of FC words received
- Crc_count - Number of frames with CRC errors

If you do not specify a value for the interval operand this command displays end to end monitor information and a cumulative count of the traffic detected by the monitor. If you specify a value for the interval operand, this command displays a snapshot of the traffic at the specified interval.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
interval	Specify an interval in seconds. This operand is optional.

Example To display end-to-end monitor frame traffic on a port at an interval of every 6 seconds:

```
switch:admin> perfshoweemonitor 4/5 6
perfshoweemonitor 53, 6: Tx/Rx are # of bytes and crc is # of crc errors
          0                1                2                3                4
 -------------    -------------    -------------    -------------    -------------
 crc   Tx   Rx    crc   Tx   Rx    crc   Tx   Rx    crc   Tx   Rx    crc   Tx   Rx
 =============    =============    =============    =============    =============
 0     0    0     0     0    0     0     0    0     0     0    0     0     0    0
 0    53m 4.9m     0    53m 4.9m     0    53m 4.9m     0    53m 4.9m     0    53m  0
 0    53m 4.4m     0    53m 4.4m     0    53m 4.4m     0    53m 4.4m     0    53m  0
 0    53m 4.8m     0    53m 4.8m     0    53m 4.8m     0    53m 4.8m     0    53m  0
 0    53m 4.6m     0    53m 4.6m     0    53m 4.6m     0    53m 4.6m     0    53m  0
 0    53m 5.0m     0    53m 5.0m     0    53m 5.0m     0    53m 5.0m     0    53m  0
 0    53m 4.8m     0    53m 4.8m     0    53m 4.8m     0    53m 4.8m     0    53m  0
 0    53m 4.5m     0    53m 4.5m     0    53m 4.5m     0    53m 4.5m     0    53m  0
 0    52m 4.5m     0    52m 4.5m     0    52m 4.5m     0    52m 4.5m     0    52m  0
 0    52m 5.0m     0    52m 5.0m     0    52m 5.0m     0    52m 5.0m     0    52m  0
 0    52m 4.5m     0    52m 4.5m     0    52m 4.5m     0    52m 4.5m     0    52m  0
 0    52m 4.6m     0    52m 4.6m     0    52m 4.6m     0    52m 4.6m     0    52m  0
```

To display EE monitors on a port:

```
switch:admin> perfshoweemonitor 4/5
    There are 7 end-to-end monitor(s) defined on port 53.
   KEY SID     DID        OWNER_APP OWNER_IP_ADDR TX_COUNT          RX_COUNT           CRC_COUNT

   ------------------------------------------------------------------------------------------------------------
   --------------
   0   0x21300   0x21dda    TELNET N/A       0x00000004d0ba9915  0x0000000067229e65  0x0000000000000000
   1   0x21300   0x21ddc    TELNET N/A       0x00000004d0baa754  0x0000000067229e65  0x0000000000000000
   2   0x21300   0x21de0    TELNET N/A       0x00000004d0bab3a5  0x0000000067229e87  0x0000000000000000
   3   0x21300   0x21de1    TELNET N/A       0x00000004d0bac1e4  0x0000000067229e87  0x0000000000000000
   4   0x21300   0x21de2    TELNET N/A       0x00000004d0bad086  0x0000000067229e87  0x0000000000000000
   5   0x11000   0x21fd6 WEB_TOOLS 192.168.169.40 0x00000004d0bade54   0x0000000067229e87
   0x0000000000000000
   6   0x11000   0x21fe0    WEB_TOOLS 192.168.169.40 0x00000004d0baed41   0x0000000067229e98
   0x0000000000000000
```

If you do not specify an interval, the EE based monitor traffic count is displayed in 64 bit format and is cumulative.

See Also `perfaddeemonitor`

perfshowfiltermonitor

Display filter-based monitor information and frame traffic for a port.

Syntax `perfshowfiltermonitor [slotnumber/]portnumber [interval]`

Availability All users

This command requires a Performance Monitor license.

Description Use this command to display all the filter-based monitors defined on the specified port and the traffic count values. This command can display (if no interval operand is specified):

- Key - the monitor number
- Alias - the monitor alias name
- Owner_app - Telnet Or Web_Tools
- Owner_ip_addr - the IP address of the owner of the filter monitor, that is, the Web Tools client.
- Frame_count - cumulative 64 bit frame count

If you do not specify a value for the interval operand, this command displays a cumulative count of the traffic detected by the monitor. If you specify a value for the interval operand, this command displays a snapshot of the traffic at the specified interval.

Operands This command has the following operand:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
interval	Specify an interval in seconds. This operand is optional.

Example **To display filter monitor traffic on a port at an interval of every 6 seconds:**

```
switch:admin> perfshowfiltermonitor 2/5 6
perfshowfiltermonitor 21, 6
   0         1          2         3         4         5         6
    #Frames    #CMDs     #CMDs    #Frames   #Frames    #CMDs     #CMDs
   ------------------------------------------------------------------
      0         0         0         0         0         0         0
     26k      187       681       682       682       494       187
     26k      177       711       710       710       534       176
     26k      184       734       734       734       550       184
     26k      182       649       649       649       467       182
     26k      188       754       755       755       567       184
     26k      183       716       716       717       534       183
     26k      167       657       656       655       488       167
     26k      179       749       749       749       570       179
     26k      164       752       752       752       588       164
     26k      190       700       700       700       510       190
     26k      181       701       701       701       520       181
     26k      200       750       750       751       550       201
     26k      180       692       692       691       512       179
     26k      179       696       696       696       517       179
     26k      187       720       720       720       533       187
     26k      200       722       722       722       522       200
     26k      204       717       717       717       513       204
```

To display filter monitor information on a port:

```
switch:admin> perfshowfiltermonitor 2/5
There are 7 filter-based monitors defined on port 21.

   KEY   ALIAS    OWNER_APP       OWNER_IP_ADDR      FRAME_COUNT
   ------------------------------------------------------------------
    0   SCSI_Frame TELNET                 N/A        0x00000000002c2229
    1   SCSI_WR    TELNET                 N/A        0x000000000000464a
    2   SCSI_RW    TELNET                 N/A        0x000000000000fd8c
    3   SCSI_RW    WEB_TOOLS       192.168.169.40    0x0000000000007ba3
    4   SCSI_RW    WEB_TOOLS      192.168.169.190    0x0000000000004f0e
    5   SCSI_RD    WEB_TOOLS       192.168.169.40    0x0000000000002208
    6   SCSI_WR    WEB_TOOLS       192.168.169.40    0x000000000000033a
   switch:admin>
```

If you do not specify an interval the filter based monitor frame count is displayed in 64 bit format and is cumulative.

See Also `perfaddusermonitor`

perfshowporteemask

Display the current end-to-end mask of a port.

Syntax `perfshowporteemask [`*slotnumber*`/]`*portnumber*

Availability All users

This command requires a Performance Monitor license.

Description Use this command to display the current end-to-end mask of a port. There are only two commands that can modify the value of the EE mask, `perfsetporteemask` and `perfcfgrestore`.

The end-to-end mask has 12 fields:

```
TxSID Domain:   on
TxSID Area:     on
TxSID ALPA:     on
TxDID Domain:   on
TxDID Area:     on
TxDID ALPA:     on
RxSID Domain:   on
RxSID Area:     on
```

```
RxSID ALPA:     on
RxDID Domain:   on
RxDID Area:     on
RxDID ALPA:     on
```

The fields that are marked on are used to trigger end-to-end monitors. The default value of the EE mask is all fields set to on.

Operands

This command has the following operand:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example

To display the end-to-end mask on a port:

```
switch:admin> perfshowporteemask 2/4
The EE mask onport 20 is set by application NONE

TxSID Domain:   on
TxSID Area:     on
TxSID ALPA:     on
TxDID Domain:   on
TxDID Area:     on
TxDID ALPA:     on
RxSID Domain:   on
RxSID Area:     on
RxSID ALPA:     on
RxDID Domain:   on
RxDID Area:     on
RxDID ALPA:     on

switch:admin>
```

See Also

`perfaddeemonitor`
`perfdeleemonitor`

```
perfshoweemonitor
perfsetporteemask
perfshowporteemask
```

pkicreate

Create pki objects

Syntax `pkicreate`

Availability Admin

Description Use this command in non-secure mode to create pki objects:

- switch private key and CSR
- private key passphrase
- install root certificate

This command does not create the switch certificate. The switch certificate should be obtained offline from Certificate Authority.

In secure mode this command will exit with a warning and will not create pki objects.

Operands None

Example **To create pki objects in non-secure mode:**

```
switch:admin> pkicreate
Installing Private Key and Csr...
Switch key pair and CSR generated...
Installing Root Certificate...
switch:admin>
```

If run in secure mode the following error message is displayed:

```
switch:admin> pkicreate

Warning !! Switch is in secure mode.
Can not create new Pki Objects. Exiting...
```

pkiremove

Remove existing pki objects.

Syntax `pkiremove`

Availability Admin

Description Use this command to remove of pki objects in non secure mode. It removes switch private key, private key passphrase, CSR, root certificate and switch certificate.

In secure mode, it displays a message and does not remove pki objects.

Operands None

Example **To remove pki objects in non-secure mode:**

```
switch:admin> pkiremove

WARNING!!!

Removing Pki objects will impair the security functionality
of this fibre channel switch. If you want secure mode enabled,
you will need to get the switch certificate again.

About to remove Pki objects.
ARE YOU SURE (yes, y, no, n): [no] y
All PKI objects removed.
switch:admin>
```

If run in secure mode the following error message is displayed:

```
switch:admin> pkiremove

This Switch is in secure mode.
Removing Pki objects is not allowed. Exiting...
```

pkishow

Display existing pki objects.

Syntax `pkishow`

Availability All users

Description Use this command to display existence of pki objects i.e. switch private key, private key passphrase, CSR, root certificate and switch certificate.

Operands None

Example **To view pki objects:**

```
switch:admin> pkishow
Passphrase       : Exist
Private Key      : Exist
CSR              : Exist
Certificate      : Empty
Root Certificate: Exist
switch:admin>
```

portalpashow

Show the ALPAs of a port.

Syntax `portalpashow [slotnumber/]portnumber`

Availability All users

Description Use this command to show the ALPAs present in a port. If the port is not an active L_port or if it does not have any AL_PA, this command prints an error.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

Example **Show the ALPAs of a port:**

```
switch:user> portalpashow 4/14
AL_PA    type            AL_PA    type            AL_PA    type
0xe2     public          0xe4     public
```

See Also `portcamshow`

portcamshow

Displays port based filter CAM utillization.

Syntax `portcamshow [slotnumber/] [portnumber]`

Availability Admin

Description Use this command to display the current filter CAM utilization of all ports or one port specified at input.

The following information is displayed:

SID used — Display total number of CAM entries used by this port. Please note that each CAM entry (either SID or DID CAM) can be shared among ports in the same quad.

DID used — Display total number of CAM entries used by this port. Please note that each CAM entry (either SID or DID CAM) can be shared among ports in the same quad.

SID entries — Display all existing Source ID entries within the CAM per quad. Please note that each CAM entry (either SID or DID CAM) can be shared among ports in the same quad.

DID entries	Display all existing Destination ID entries within the CAM per quad. Please note that each CAM entry (either SID or DID CAM) can be among ports in the same quad.
SID Free	Display the total number of free SID CAM entries per quad.
DID Free	Display the total number of free DID CAM entries per quad.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

Example To display the filter CAM utilization for all ports on a switch:

```
switch:admin> portcamshow
Ports of Slot 9
------------------------
Port  SID used  DID used
 0       0          0
 1       0          0
 2       0          0
 3       0          0
 4       0          0
 5       0          0
 6       0          0
 7       0          0
 8       0          0
 9       0          0
10       0          0
11       0          0
12       0          0
13       0          0
14       0          0
15       0          0
------------------------
Quad ports (SID Free, DID Free)
00-03 (64, 512) 04-07 (64, 512) 08-11 (64, 512) 12-15 (64, 512)
<output truncated>
```

To display the filter CAM utilization for a single port on a switch:

```
switch:admin> portcamshow 3/2
-------------------------------------------------
Area  SID used  DID used  SID entries  DID entries
34       3         1       350400       2b2200
                                        2b1200
                                        220400
-------------------------------------------------
Quad ports (SID Free, DID Free)
32-35 (61, 511)
switch:admin>
```

See Also switchshow

portcfgdefault

Restore the port configuration to default values.

Syntax `portcfgdefault [slotnumber/]portnumber`

Availability Admin

Description Use this command to reset any special configuration values on a port to their factory defaults. You can view the current port configuration using the `portcfgshow` command.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To reset a port to factory defaults:**

```
switch:admin> portcfgdefault 1/3
done.
```

See Also

```
portcfgshow
portcfgeport
portcfggport
portcfglport
portcfglongdistance
portcfgspeed
portcfgtrunkport
portcfgpersistentdisable
portcfgpersistentenable
```

portcfgeport

Enable or disable a port from becoming an E_Port.

Syntax `portcfgeport [slotnumber/]portnumber, mode`

Availability Admin

Description Use this command to enable or disable a port from becoming an E_Port. The E_Port capability is enabled by default unless this command is used to disable it.

When a port is configured as a non-E_Port through this command, an ISL connected to this port will be segmented. No data traffic between two switches will be routed through this port. Fabric management data, such as zoning information, will not be exchanged through this port either.

Regardless of how many E_ports are connected between two switches, the maximum routing paths are currently limited to 8 E ports.

The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

mode Specify 1 to enable the port to become an E_Port. This is the default port state. Specify 0 to disable the port from becoming an E_Port. When the *portnumber* operand is present, this operand must also be present.

When no operands are specified, the command displays the command syntax.

Example

To disable a port from becoming an E_Port:

```
switch:admin> portcfgeport 2/3, 0
Committing configuration...done.
```

See Also

```
portshow
switchshow
```

portcfggport

Designate a port as a locked G_Port.

Syntax

```
portcfggport [slotnumber/]portnumber, mode
```

Availability

Admin

Description

Use this command to designate a port as a locked G_Port. Once this is done, the switch attempts to initialize that port as an F_Port only, and does not attempt loop initialization (FL_Port) on the port. However, if the device attached to the port initiates loop communication, then the switch responds accordingly and the port can then become an FL_Port. Similarly, a port designated as a G_Port can become an E_Port.

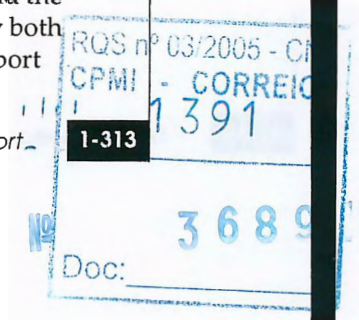
Locking a port as a G_Port only changes the actions initiated by the switch; it does not change how the switch responds to initialization requests.

The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

Operands

This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port



number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

mode Specify a value of 1 to designate the port as a G_Port or specify a value of 0 to remove the G_Port designation from the port. A value of 0 is the default port state. This operand is required.

Example

To configure a port as a locked G_Port:

```
switch:admin> portcfggport 2/3, 1
done.
```

See Also

`portshow`
`switchshow`
`configure`
`portcfgshow`

portcfgislmode

Enable or disable ISL R_RDY Mode on a port.

Syntax

`portcfgislmode [slotnumber/]portnumber, [1 | 0]`

Availability

Admin

Description

Use this command to enable or disable ISL R_RDY Mode on a port. If enabling ISL R_RDY Mode on a port make sure the PID format is consistent across the entire fabric. Refer to the `configure` command for more information on the Core PID format.

ISL R_RDY Mode sends ELP with Flow Control Mode 02 and enables connectivity with WAN gateway products. If a port is ISL R_RDY mode enabled, it can only receive ELP with Flow Control Mode 02; ELP with Flow Control Mode 01 will segment the fabric.

This mode cannot detect the PID format of connected ports. If the PID formats for two ISL R_RDY mode ports are not the same, zoning will drop frames.

This feature is persistent across reboots, and does not require a license key.

Use the `portcfgshow` command to view whether ISL R_RDY mode is enabled on a port.

Operands

This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
`[1 | 0]`	Specify 1 to enable ISL R_RDY mode. Specify 0 to disable ISL R_RDY mode. This operand is required.

Example

To enable ISL R_RDY mode on a port:

```
switch:admin> portcfgislmode 2/3, 1
Committing configuration...done.
ISL R_RDY Mode is enabled for port 3. Please make sure the PID
formats are consistent across the entire fabric.
switch:admin>
```

To disable ISL R_RDY mode on a port:

```
switch:admin> portcfgislmode 2/3, 0
Committing configuration...done.
switch:admin>
```

See Also `portcfgshow`

portcfglongdistance

Configure a port to support long distance links.

Syntax `portcfglongdistance [slotnumber/]portnumber [ distance_level] [vc_translation_link_init]`

Availability Admin

This command requires an Extended Fabric license.

Description Use this command to allocate enough full size frame buffers on a particular port to support a long distance link up to 100km. The port can only be used as an E_Port. The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

The value of *distance_level* can be one of the following (the numerical value representing each *distance_level* is shown in parentheses):

- `L0` (0): Re-configure the port to be a regular switch port. The number of buffers reserved for the port supports up to 10km links.
- `L0.5`: Level 0.5 (`switchshow` and `portcfgshow` show two letter code as LM) long distance, up to 25km. A total of 15 or 30 full size frame buffers will be reserved for the port at speeds of 1 Gbit/sec and 2 Gbit/sec respectively.
- `L1` (1): Level one long distance, up to 50km. A total of 24 or 50 full size frame buffers will be reserved for the port at speeds of 1 Gbit/sec and 2 Gbit/sec respectively.
- `L2` (2): Level two long distance, up to 100km. A total of 58 or 63 full size frame buffers will be reserved for the port at speeds of 1 Gbit/sec and 2 Gbit/sec respectively.
- `LE` (3): Level E mode is for E ports for distances beyond 5km and up to 10km especially for 2G link speeds. A total of 7 or 13 full size frame buffers will be reserved for the port at speeds of 1 Gbit/sec and 2 Gbit/sec respectively. LE does not require extended fabric license.

- LD: Dynamic long distance configuration. The buffer credits for the given E-port are automatically configured based on the actual link distance. Up to a total of 63 full size frame buffers will be reserved depending upon the distance measured during E-port initialization.

The option `VC Translation Link Init` is used to enable the long distance link initialization sequence. By default this option is set to 0 (disabled).

An input of CTRL-D cancels the configuration update.

When a port is configured to be a long distance port, the output of `portshow` and `switchshow` will print the long distance level. In the `portshow` output, the long distance level is indicated as follows,

- L0 normal
- LE standard <= 10km
- LM medium long <= 25km
- L1 long <= 50km
- L2 super long <= 100km
- LD auto-detect

In the `switchshow` output, the long distance mode is displayed as `Lx`, where x is the second letter in two letter distance level code described above.

Refer to the *Brocade Distributed Fabrics User's Guide* for more information.

Trunking is not supported with LE, L1, and L2 `portcfglongdistance` modes. Trunking is supported for normal E_Ports (referred to as L0 in `portcfglongdistance` command) with LWL media up to 5km at the full speed permitted by the link. With LWL media, the throughput begins to fall off beyond 5km, due to normal latency effects.

Operands This command has the following operands:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

distance This operand indicates the distance to the connected port. This operand is required. The valid values for this operand are:

- L0: Re-configure the port to be a regular switch port. The number of buffers reserved for the port supports up to 10km links.
- LE: Level E mode is for E ports for distances beyond 5km and up to 10km especially for 2G link speeds.
- L0.5 (LM): Level 0.5 long distance, up to 25km.
- L1: Level one long distance, up to 50km. A total of 26 full size frame buffers will be reserved for the port.
- L2: Level two long distance, up to 100km. A total of 60 full size frame buffers will be reserved for the port.
- LD: Automatic long distance configuration.

VC_Translation_Link_Init
Specify 1 to activate long distance link initialization sequence. Specify 0 to deactivate this mode. The default value is 0 (disabled). This operand is optional.

Limitations Since the total number of frame buffers is shareable on a quad base, when one of the ports in the quad is configured as a long distance port, the remaining ports could be disabled due to lack of frame buffers. If a port is configured as long distance port and there is not enough frame buffers left in that quad, the port will not be initialized.

A quad is defined as a group of four adjacent ports that share a common pool of frame buffers. For example, ports 0-3 belong to a quad, ports 4-7, and so on.

Refer to the *Brocade Distributed Fabrics User's Guide* for more information on limitations in port configurations.

Example **To configure a port to support a 100km link and be initialized using long distance link initialization protocol:**

```
switch:admin> portcfglongdistance 4/15 L2 1
done.
switch:admin> portshow 4/15
portCFlags: 0x1
portFlags: 0x20001       PRESENT LED
portType:  1.1
portState: 2    Offline
portPhys:  4    No_Light
portScn:   0
portId:    013f00
portWwn:   20:3f:00:60:69:00:02:48
Distance:  super long <= 100km
portSpeed: 2Gbps

Interrupts:        9          Link_failure: 0          Frjt:          0
Unknown:           0          Loss_of_sync: 0          Fbsy:          0
Lli:               9          Loss_of_sig:  9
Proc_rqrd:         0          Protocol_err: 0
Timed_out:         0          Invalid_word: 0
Rx_flushed:        0          Invalid_crc:  0
Tx_unavail:        0          Delim_err:    0
Free_buffer:       0          Address_err:  0
Overrun:           0          Lr_in:        0
Suspended:         0          Lr_out:       0
Parity_err:        0          Ols_in:       0
2_parity_err:      0          Ols_out:      0
CMI_bus_err:       0
```

See Also

```
configure
portcfgshow
portshow
switchshow
```

portcfglport

Lock a port as an L_PORT.

Syntax `portcfglport [slotnumber/]portnumber, lockmode[, privatemode]`

Availability Admin

Description Use this command to designate a port as an L_PORT. The switch will then only attempt to initialize that port as an FL_PORT. The switch never attempts point-to-point (F_PORT) initialization on the port. However, if the device attached to the port initiates point-to-point communication, then the switch will respond accordingly, and the port may then become an F_PORT.

Similarly, being locked as an L_PORT will not prevent the port from becoming an E_PORT. Locking a port as an L_PORT only affects what actions the switch initiates. It does not change how the switch responds to initialization requests.

Operands This command has the following operands:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

lockmode Specify 1 to configure the specified port as a locked L_PORT. Specify 0 to de-configure the specified port from its previous role as a locked L_PORT. This operand is required.

privatemode Specify 1 to configure the L_PORT as a private L_PORT (then FLOGI will be rejected). Specify 0 to configure the L_PORT as a normal public L_PORT. The default value is 0. This operand is optional.

Example

To configure a port as a locked L_PORT:

```
switch:admin> portcfglport 2/3, 1
done.
```

See Also

`portshow`
`switchshow`
`configure`

portcfgpersistentdisable

Disable a port persistently.

Syntax `portcfgpersistentdisable` *portnumber*

Availability Admin

Description Use this command to persistently disable a port. Persistently disabled ports remain disabled across power cycles, switch reboots, and switch enables. By default a port is enabled persistently. The change in configuration is effective immediately.

The persistent disable configuration overrides all other port configurations but it does not change the configuration of any other port settings. Use the `portcfgpersistentenable` command to enable a port persistently. A persistent enabled port re-enables all previously set port configurations of that port.

The switch will still run the power on diagnostics and initialize a persistently disabled port. A persistently disabled port can temporarily be enabled by `portenable` command. The `switchenable` command will not enable the persistently disabled ports of that switch.

The persistent switch disable or enable configuration does not alter the persistent disable or enable configurations of the ports within the switch.

Like all other configurable port attributes, port persistent disable will not be affected by `configdefault` command. But it will be cleared by `portcfgdefault` command, because a port, by default, is enabled persistently.

Operands This command has the following operands:

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

When no operand is specified, the command reports the current port persistent disable status for all ports in the switch. The value of YES is displayed for ports that are persistently disabled.

Example **To configure a port as persistently disabled:**

```
switch:admin> portcfgpersistentdisable 9/3
switch:admin> portcfgpersistentdisable
Slot 9     0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15
---------+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---
Disabled   -   -   -  YES  -   -   -   -   -   -   -   -   -   -   -   -

switch:admin>
```

See Also `portcfgpersistentenable`
`portcfgshow`
`portshow`
`switchshow`
`configure`
`configshow`
`configdefault`
`portcfgdefault`

portcfgpersistentenable

Enable a port persistently.

Syntax `portcfgpersistentenable` *portnumber*

Availability Admin

Description Use this command to persistently enable a port. Persistently enabled ports remain enabled across power cycles, switch reboots, and switch enables. By default a port is enabled persistently. The change in configuration is effective immediately.

A persistent port enable will re-enable all previously set port configurations of that port. A persistently enabled port can temporarily be disabled by `portdisable` or `switchdisable`

command. The `switchdisable` command will also disable the persistently enabled ports of that switch.

The persistent switch disable or enable configuration does not alter the persistent disable or enable configurations of the ports within the switch.

The configuration commands, `configdefault` and `portcfgdefault`, do not modify the persistent enable attribute of a port.

Operands

This command has the following operands:

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

When no operand is specified, the command reports the current port persistent enabled status for all ports in the switch. The value of YES is displayed for ports that are persistently enabled.

Example

To configure a port as persistently enabled:

```
switch:admin> portcfgpersistentenable 9/3
switch:admin> portcfgpersistentenable
Slot 9      0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15
---------+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---
Enabled    YES YES YES YES YES YES YES YES YES YES YES YES YES YES YES YES

switch:admin>
```

See Also

`portcfgpersistentdisable`
`portcfgshow`
`portshow`
`switchshow`
`configure`
`configshow`
`portcfgdefault`
`configdefault`

portcfgshow

Display port configuration settings.

Syntax `portcfgshow [slotnumber/] [portnumber]`

Availability All users

Description Use this command to display the current configuration of all ports. If no operand is specified, all the port configuration settings are displayed for that switch, or for the ED-12000B logical switch.

The following configuration information is displayed:

- `Speed` mode is displayed as 1G, 2G, or AN (when in Auto speed Negotiation mode). This value is set by the `portcfgspeed` command.
- `Trunk Port` mode is displayed as ON when port is set for trunking or blank (..) when trunking is disabled on the port. This value is set by the `portCfgTrunkport` command.
- `Long Distance` mode is displayed as blank (..) when long distance mode is off, L1 when the link is up to 50Km, or L2 when the link is up to 100Km. This value is set by the `portcfglongdistance command`.
- `VC Link Init` mode (virtual channel) is displayed as blank (..) when the long distance link initialization option is turned off and (ON) when it is turned on for long distance mode. This value is set by the `portcfglongdistance` command.
- `Locked L_Port` mode is displayed as ON when port is locked to L_Port only or blank (..) when L_Port lock mode is disabled (and it behaves as a U_Port). This value is set by the `portcfglport` command.
- `Locked G_Port` mode is displayed as ON when port is locked to G_Port only or blank (..) when G_Port lock mode is disabled (and it behaves as a U_Port). This value is set by the `portcfggport` command.
- `Disabled E_Port` mode is displayed as ON when port is not allowed to be an E_Port or blank (..) when the port is allowed to function as an E_Port. This value is set by the `portcfgeport` command.

- Mcast LoopBack mode is displayed as blank (..) when Mcast LoopBack mode is off, and (ON) when Mcast LoopBack mode is enabled. This value is set by the portcfgmcastloopback command.
- `ISL R_RDY` mode is displayed as ON when the port has been R_RDY mode enabled or blank (..) when the port is allowed to function as an E_Port. This value is set by the `portcfgislmode` command.
- `Persistent Disable` mode is displayed as ON when the port is disabled across reboots or power cycles or (..) when the port is allowed to function normally. This value is set by the `portcfgpersistentdisable` command.

Operands This command has the following operands:

`slotnumber`	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
`portnumber`	Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

Example To display the configuration settings of ports in a DS-32B2:

```
switch:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed              AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port         ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init       .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port    .. ON .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Mcast LoopBack     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..

Ports of Slot 0   16 17 18 19   20 21 22 23   24 25 26 27   28 29 30 31
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed              AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port         ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init       .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Mcast LoopBack     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..

                  where AN:AutoNegotiate, ..:OFF, ??:INVALID.
                        LM:L0.5
switch:admin> portcfgshow 15
Area Number:               15
Speed Level:               AUTO
Trunk Port                 ON
Long Distance              OFF
VC Link Init               OFF
Locked L_Port              OFF
Locked G_Port              OFF
Disabled E_Port            OFF
Mcast LoopBack             OFF
ISL R_RDY Mode             OFF
Persistent Disable         OFF

switch:admin>
```

See Also

```
portcfgeport
portcfggport
portcfglport
portcfglongdistance
portcfgtrunkport
```

portcfgspeed

portcfgspeed

Configure the port speed level.

Syntax `portcfgspeed [slotnumber/]portnumber, speed_level`

Availability Admin

Description Use this command to configure the speed of a port to a particular level. After this command is issued, the port is disabled and enabled so that the port comes up with the new speed setting. The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

If the command is specified without an operand, you are prompted to enter the speed value.

The output of the `portshow` command displays the current achieved speed of a port and the `portcfgshow` command displays the user desired speed setting for a port.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
speed_level	Specify the speed of a port. This operand is required. Valid values are one of the following:

0 Auto-sensing mode. The port automatically configures for the highest speed.

1 1 Gbit/sec mode. The port will be at fixed speed of 1 Gbit/sec.

2 2 Gbit/sec mode. The port will be at fixed speed of 2 Gbit/sec.

Example **To configure the speed of a port to 2 Gbit/sec:**

```
switch:admin> portcfgspeed 2/5, 2
done.
```

See Also

```
switchcfgspeed
portshow
```

portcfgtrunkport

Configure a port to be enabled or disabled for trunking.

Syntax `portcfgtrunkport [slotnumber/]portnumber, mode`

Availability Admin

This command requires a Trunking license.

Description Use this command to enabled or disabled a port for trunking.

Operands This command has the following operand:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

mode Specify 1 to enable this port for trunking. Specify 0 to disable this port for trunking. This operand is required.

Example **To enable a port for trunking:**

```
switch:admin> portcfgtrunkport 1/3, 1
done.
```

See Also

```
switchcfgtrunk
portshow
portcfgshow
switchshow
```

portdebug

Set debug level and verbose level of port modules.

Syntax `portdebug dbg_lvl, vbs_lvl`

Availability Admin

Description Use this command to set the debug level and verbose level of port modules.

Operands This command has the following operands:

dbg_lvl Specify the debug level to be set for port modules. Valid values are 1 - 5.

vbs_lvl Specify the verbose level to be set for port modules. Valid values are 1 - 5.

Example **To set debug level and verbose level of port modules:**

```
switch:admin> portdebug 3, 4
```

See Also `dbgshow`

portdisable

Disable a switch port.

Syntax `portdisable [slotnumber/]portnumber`

Availability Admin

Description Use this command to disable a switch port. If the port is connected to another switch, the fabric may reconfigure. If the port is connected to one or more devices, the devices can no longer communicate with the fabric.

If the port was online before being disabled, a state transition will be indicated in the following ways: RSCN, SNMP trap, Web pop-up window.

The front panel LED of a disabled port flashes yellow with a two second cycle.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example

To disable a port in a ED-12000B:

```
switch:admin> portdisable 2/4
```

To disable a port in a DS-32B2:

```
switch:admin> portdisable 4
```

See Also `portenable`

```
portcfgpersistentdisable
portcfgpersistentenable
portshow
switchshow
```

portenable

Enable a switch port.

Syntax `portenable [slotnumber/]portnumber`

Availability Admin

Description Use this command to enable a switch port. If the port is connected to another switch, the fabric may reconfigure. If the port is connected to one or more devices, the devices can communicate with the fabric.

For ports that come online after being enabled, the following indications may be sent to indicate a state transition: RSCN, SNMP trap, Web pop-up window.

The front panel LED of an enabled and online port is green.

Operands This command has the following operand:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To enable a port in a ED-12000B:**

```
switch:admin> portenable 2/4
switch:admin>
```

To enable a port in a DS-32B2:

```
switch:admin> portenable 4
switch:admin>
```

See Also

```
portdisable
portcfgpersistentdisable
portcfgpersistentenable
portshow
switchshow
```

porterrshow

Display port error summary.

Syntax

```
porterrshow
```

Availability

All users

Description

Use this command to display an error summary for all ports. The display contains one output line per port and shows error counters in ones, thousands (K), or millions (M).

The following fields are displayed:

frames tx	Frames transmitted.
frames rx	Frames received.
enc in	Encoding errors inside frames.
crc err	Frames with CRC errors.
too shrt	Frames shorter than minimum.
too long	Frames longer than maximum.
bad eof	Frames with bad end-of-frame delimiters.
enc out	Encoding error outside of frames.
disc c3	Class 3 frames discarded.
link fail	Link failures (LF1 or LF2 states).

buffers (per-port)
credits (per-port)
data (per-port)
phantom (per-port)
properties (per-port)
statistics (per-port)

- filter (DISABLED by default). This group has lengthy output.

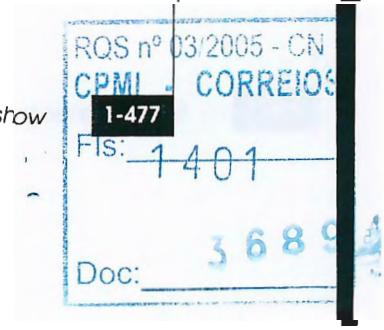
  `filterportshow` (per-port)

- perfmon (DISABLED by default).

  `ps_dump` (per-port) The output of this command can be very long.

Operands This command has the following operands:

`slotnumber`	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of ten slots. Slot number 5 and 6 are control processor cards, and slots 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
`port1`	Specify the first port of a range of ports to display information. Enter the port area number. Both *`port1`* and *`port2`* must be provided if a range of ports is specified. For the ED-12000B, a slot number is required if a port-range is specified. If no range is specified, then all the ports for the slot or switch are specified.
`port2`	Specify the last port in the range of ports to display information. Enter the port area number. Both *`port1`* and *`port2`* must be provided if a range of ports is specified.ED-12000B
`lines`	Specify the number of lines of `portlogdump` output displayed. This operand is optional.



Example To display switch information for debugging:

```
switch:admin> supportshow 1/1-3
supportshow groups enabled: system
version:
Kernel:      2.4.19
Fabric OS:   v4.1.0
Made on:     Fri Jan 10 01:06:10 2003
Flash:       Thu Jan 17 00:06:52 2003
BootProm:    3.2.1

uptime:
 10:49am  up  3:25,  1 user,  load average: 1.55, 1.20, 1.11

switchshow:
switchName:      switch
switchType:      10.1
switchState:     Online
switchMode:      Native
switchRole:      Principal
switchDomain:    1
switchId:        fffc01
switchWwn:       10:00:00:60:69:80:03:0c
zoning:          OFF
switchBeacon:    OFF
blade1 Beacon:   OFF

---<output truncated>---
```

See Also `supportshowcfgdisable`
`supportshowcfgenable`
`supportshowcfgshow`

supportshowcfgdisable

Disable a group of commands under the `supportshow` command.

Syntax `supportshowcfgdisable [os | exception | port | fabric | services | security | network | portlog | system extend | filter | perfmon]`

Availability Admin

Description Use this command to disable a group of commands under the `supportshow` command. Use the `supportshowcfgenable` command to enable groups of commands. Refer to Chapter 7, *Supportshow Reference*, for more information

Operands This command has the following operand:

commgroup Specify a command group to disable that group from displaying under the `supportshow` command. The operand must be entered exactly as shown. At least one group must be specified. The groups are as follows:

- os
- exception
- port
- fabric
- services
- security
- network
- portlog
- system
- extend
- filter
- perfmon

Example **To disable the os group of commands under the supportshow command:**

```
switch:admin> supportshowcfgdisable os
Config update Succeeded
```

See Also

```
supportshow
supportshowcfgenable
supportshowcfgshow
```

supportshowcfgenable

Enable a group of commands under the **supportshow** command.

Syntax

```
supportshowcfgenable [os | exception | port | fabric |
services | security | network | portlog | system
extend | filter | perfmon]
```

Availability Admin

Description Use this command to enable a group of commands under the `supportshow` command. Use the `supportshowcfgdisable` command to disable groups of commands. Refer to Chapter 7, *Supportshow Reference*, for more information

Operands This command has the following operands:

commgroup Specify a command group to enable that group to display under the `supportshow` command. The operand must be entered exactly as shown. Only one group can be specified. The groups are as follows:

- os
- exception
- port
- fabric
- services
- security
- network
- portlog
- system
- extend
- filter
- perfmon

Example **To enable a group of commands under the supportshow command:**

```
switch:admin> supportshowcfgenable os
Config update Succeeded
```

See Also

```
supportshow
supportshowcfgdisable
supportshowcfgshow
```

supportshowcfgshow

Display the groups of commands enabled for display by the `supportshow` command.

Syntax `supportshowcfgshow`

Availability Admin

Description Use this command to display the groups of commands enabled for display by the `supportshow` command. Use the `supportshowcfgenable` and the `supportshowdisable` commands to modify which groups are displayed. Refer to Chapter 7, *Supportshow Reference*, for more information

Operands None

Example To display which groups of commands are enabled in the supportshow command:

```
switch:admin> supportshowcfgshow
 os          enabled
 exception   enabled
 port        enabled
 fabric      enabled
 services    enabled
 security    enabled
 network     enabled
 portlog     enabled
 system      enabled
 extend      disabled
 filter      disabled
 perfmon     disabled
switch:admin>
```

See Also

```
supportshow
supportshowcfgdisable
supportshowcfgenable
```

switchbeacon

Set switch beaconing mode on or off.

Syntax `switchbeacon [mode]`

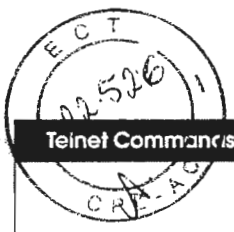
Availability Admin

Description Use this command to enable or disable the switch beaconing mode. When beaconing mode is turned on, the port LEDs flash amber in a running pattern. The user sees a running pattern in amber LEDs, from left to right and right to left. The pattern continues until turned off by the user.

Beaconing mode affects only the port LEDs. Other commands are still executable and functional. The normal flashing LED pattern (associated with an active, faulty or disabled port) is suppressed and the beaconing pattern is shown. However, if diagnostic frame based tests (`portloopbacktest`, `crossporttest`, and `spinsilk`) are executed, two patterns are interleaved. The diagnostic test flickers the LEDs green and simultaneously the beaconing mode runs the LEDs amber.

Use the `switchshow` command to display the status of beaconing.

Operands This command has the following operand:



mode Specify 1 to enable beaconmode or 0 to disable beaconmode. This operand is optional.

If no operand is specified the current value is displayed.

Example

To turn beaconing mode ON:

```
switch:admin> switchbeacon 1
```

To turn beaconing mode OFF:

```
switch:admin> switchbeacon 0
```

See Also `switchshow`

switchcfgpersistentdisable

Disable switch persistently.

Syntax `switchcfgpersistentdisable`

Availability Admin

Description Use this command to persistently disable the switch. The persistently disabled switch remains disabled across power cycles and switch reboots. It will not participate in fabric reconfiguration and will remain isolated from the rest of the topology. By default a switch is enabled persistently.

When this command is executed, it will become effective immediately by disabling the switch, if it is not already disabled.

The persistent switch disable configuration overrides all other switch configurations but it does not alter any of them. The `switchcfgpersistentenable` command will enable the switch persistently. The persistent switch enable will also re-enable all previously set switch configurations.

The persistent switch disable configuration will override port persistent enable configurations but it will not alter them.

The persistently disabled switch will still run the power on diagnostics and initialize all the ports.

A persistently disabled switch can temporarily be enabled by `switchenable` command until next switch disable, power cycle or switch reboot.

Operands None

Example **To disable a switch persistently:**

```
switch:admin> switchcfgpersistentdisable
Committing configuration...done.
Command in progress . . . . . done
```

See Also

```
switchcfgpersistentenable
portcfgshow
portshow
switchshow
configure
configshow
portcfgpersistentdisable
portcfgpersistentenable
```

switchcfgpersistentenable

Enable a switch persistently.

Syntax `switchcfgpersistentenable`

Availability Admin

Description Use this command to persistently enable the switch. The persistently enabled switch remains enabled across power cycles and switch reboots. By default a switch is enabled persistently.

When this command is executed, it will be effective immediately by enabling the switch, if it is not already enabled.

The persistent switch disable configuration overrides all other switch configurations but it does not alter any of them. The persistent switch enable will also re-enable all previously set switch configurations.

A persistently enabled switch can temporarily be disabled by `switchdisable` command until next switch enable, power cycle or switch reboot.

The persistent switch disable or enable configuration does not alter the persistent disable or enable configurations of the ports within the switch.

Operands None

Example The following example configures the switch as persistently enabled:


```
switch:admin> switchcfgpersistentenable
Committing configuration...done.
Command in progress . . . . . done
```

See Also

```
switchcfgpersistentdisable
portcfgshow
portshow
switchshow
configure,
configshow
portcfgpersistentdisable
portcfgpersistentenable
```

switchcfgspeed

Configure all ports of the switch to a particular speed level.

Syntax `switchcfgspeed` *`speed_level`*

Availability Admin

Description Use this command to configure the speed of all the ports on a switch to a particular level. The configuration is saved in the non-volatile memory and persists across switch reboot or power cycle.

The output of `portshow` and `portcfgshow` displays the speed level. In the `portshow` output, the speed level is indicated as the current port speed of `1Gbs` or `2Gbs`. In the `portcfgshow` output, the speed level is indicated as `1G`, `2G`, or `AN` (Auto-Negotiate).

Operands This command has the following operand:

`speed_level` Specify the speed of a port. This operand is required. Valid values are one of the following:

- 0 Auto-sensing mode. The port automatically configures for the highest speed.
- 1 1 Gbit/sec mode. The port will be at fixed speed of 1 Gbit/sec.
- 2 2 Gbit/sec mode. The port will be at fixed speed of 2 Gbit/sec.

Example **To set the speed level for all ports on a switch:**

```
switch:admin> switchcfgspeed 2
done.
switch:admin>
```

See Also `portcfgspeed`
`switchshow`

switchcfgtrunk

Enable or disable trunking on all the ports of a switch.

Syntax `switchcfgtrunk` *mode*

Availability Admin

This command requires the Trunking license.

Description Use this command to enable or disable trunking on all the ports of a switch.

Operands This command has the following operand:

mode	Specify 1 to enable trunking on all the ports on this switch. Specify 0 to disable trunking on all the ports on this switch. This operand is required.

Example **To enable trunking on a switch:**

```
switch:admin> switchcfgtrunk 1
done.
```

See Also `portcfgtrunkport`
`portshow`
`portcfgshow`
`switchshow`

switchdiag

Run a suite of diagnostic tests on a switch.

Syntax `switchdiag [-log logfile]`

Availability Admin

Description Use this command to run a suite of diagnostic tests on the specified switch (fixed port count products only).

This command executes the following commands:

- portregtest

- centralmemorytest
- cmitest
- camtest
- filtertest
- statstest
- portloopbacktest
- txdpath
- crossporttest
- turboramtest
- spinsilk
- backport
- diagshow

Each diagnostic test in this suite may report its own set of error messages when it detects failures. Refer to the *Errors* section of the individual commands.

To run this test, you must install loopback plugs on every port. Run `systemtest` otherwise.

Options This command has the following options:

`-log` *`logfile`* Specify that the output of the command will be placed in a file named by the *`logfile`* argument. The log file will contain all activity that occurred during the execution of the command. All error messages are also saved in the logfile. If this option is not specified, no log file is created.

Example **To run a suite of diagnostics on a switch:**

```
switch:admin> switchdiag
Testing user ports: 0 1 2 3 4 5 6 7 8 9 10 .     .

portregtest

Running portregtest ..............
Test Complete: "portregtest" Pass 1 of 1
Duration 0 hr, 2 min & 14 sec (0:2:14:659)
 passed.

centralmemorytest

Running centralmemorytest ............
Test Complete: "centralmemorytest" Pass 1 of 1
Duration 0 hr, 0 min & 18 sec (0:0:18:415)
 passed.
```

```
--- <output truncated> ---
```

See Also

```
backport
bladediagshort
switchdiag
switchdiagshort
camtest
centralmemorytest
cmitest
crossporttest
diagshow
filtertest
portloopbacktest
portregtest
spinsilk
statstest
systemtest
turboramtest
txdpath
```

switchdiagshort

Run diagnostics on a switch blade.

Syntax `switchdiag [-log logfile]`

Availability Admin

Description Use this command to run a suite of diagnostic tests on the specified switch (fixed port count products only). This command executes the following commands:

- portregtest
- centralmemorytest
- cmitest
- camtest
- filtertest
- statstest
- portloopbacktest
- txdpath
- crossporttest
- turboramtest
- spinsilk
- backport
- diagshow

Each diagnostic test in this suite may report its own set of error messages when it detects failures. Refer to the *Errors* section of the individual commands.

To run this test, you must install loopback plugs on every port. Run `systemtest` otherwise.

Options

This command has the following options:

`-log` *`logfile`* Specify that the output of the command will be placed in a file named by the *`logfile`* argument. The log file will contain all activity that occurred during the execution of the command. All error messages are also saved in the logfile. If this option is not specified, no log file is created.

Example

To run a suite of diagnostics on a switch:

```
switch:admin> switchdiagshort
Testing user ports: 0 1 2 3 4 5 6 7 8 9 10 ......

portregtest

Running portregtest ..............
Test Complete: "portregtest" Pass 1 of 1
Duration 0 hr, 2 min & 14 sec (0:2:14:655).
 passed.

centralmemorytest

Running centralmemorytest ............
Test Complete: "centralmemorytest" Pass 1 of 1
Duration 0 hr, 0 min & 18 sec (0:0:18:415).
 passed.
--- <output truncated> ---
```

See Also

```
backport
bladediag
switchdiag
switchdiagshort
camtest
centralmemorytest
cmitest
crossporttest
diagshow
filtertest
portloopbacktest
portregtest
spinsilk
```

```
statstest
systemtest
turboramtest
txdpath
```

switchdisable

Disable the switch.

Syntax `switchdisable`

Availability Admin

Description Use this command to disable the switch. All fibre channel ports are taken offline; if the switch was part of a fabric, the remaining switches reconfigure.

The switch must be disabled before making configuration changes (using `configure` or `configdefault`) or before running many of the diagnostic tests. All commands that require the switch to be disabled send an error if invoked while the switch is enabled.

The switch does not need to be disabled before rebooting or powering off.

As each port is disabled, the front panel LED changes to a slow flashing yellow.

Operands None

Example **To disable the switch:**

```
switch:admin> switchdisable
```

See Also

```
switchenable
switchshow
```

switchenable

Enable the switch.

Syntax `switchenable`

Availability Admin

Description Use this command to enable the switch. All fibre channel ports that passed POST are enabled. They can come online if connected to a device, or remain offline if disconnected. A switch may need to be enabled if it was previously disabled to make configuration changes or to run diagnostics.

If the switch is connected to a fabric, it rejoins the fabric. When this command is issued, the 10 second fabric stability count down is displayed. If this switch remains the principal switch at the end of the count down, then it assigns itself a domain ID. If another switch assumes the principal role, then this switch becomes a subordinate switch, and accepts a domain ID from the principal. See FC-SW for a complete description of this process.

As each port is enabled, the front panel LED changes to green for online ports, black for disconnected ports, or yellow for un-initialized ports.

Operands None

Example **To enable a switch:**

```
switch:admin> switchenable
10  9  8  7  6  5  4  3  2  1
fabric: Principal switch
fabric: Domain 1
```

See Also

```
switchdisable
switchshow
```

switchname

Display or set the switch name.

Syntax `switchname ["newname"]`

Availability All users (display)

Admin (set)

Description Use this command to display or set the switch name. All switches have a symbolic name that is primarily used for switch management. This name is also shown in the Fabric OS CLI prompt, under each switch icon on the Fabric Web page, and in the output of various Fabric OS commands, such as `fabricshow`.

Enter this command with no operand to display the current switch name.

Use this command with the *newname* operand to assign a new switch name. Switch names can be up to 15 characters long, must begin with an alpha character, and can consist of any combination of alphanumeric, and underscore characters.

Changing the switch name causes a domain address format RSCN to be issued (see FC-FLA for a description of RSCNs).

The switch's name may also be changed using Web Tools.

Operands This command has the following operand:

newname	Specify a new name for the switch, in quotation marks. This operand is optional.

Example **To change a switch name to sw10:**

```
switch:admin> switchname "sw10"
Committing configuration...
Done.
sw10:admin>
```

See Also

```
switchshow
fabricshow
```

switchreboot

Halt and bring down the operational switch.

Syntax `switchreboot`

Availability Admin

Description This command reboots the operational switch without disrupting the other switch in the ED-12000B chassis. This command will be used by the administrator when he can not determine the problem with the switch and want to bring it back to an operational state with out disturbing the software state of the system in general.

This command is equal to running `switchshutdown` and `switchstart`.

For the ED-12000B, the `switchreboot` command will reboot only the logical switch you are currently logged into, the other logical switch and both CPs remain unaffected.

Operands None

Example To bring down an operational switch:

```
switch:admin> switchreboot
Selecting i2c bus...Done.
Stopping all switch daemons...Done.
Releasing i2c bus...Done.
Powering off slot 7...Done.
Checking all slots are powered off....Done.
Cleaning up kernel modules...Done.
Initializing kernel modules...Done.
setup FCIP IP: ifconfig fc1 ip=192.168.69.190, netmask=255.255.255.0
Starting all switch daemons...Done.
Powering on slot 7...Done.
Checking diagnostics..............
Start Apache -- /etc/rc.d/init.d/httpd.sh start 1 192.168.174.95
   192.168.69.190
Start snmpd -- /etc/rc.d/init.d/snmpd.sh start 1
starting http server [1] ...
.Starting snmpd:\n
SNMP Research SNMP Agent Resident Module Version 15.2.1.3
Copyright 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999
   SNMP
Research, Inc..
/fabos/webtools/bin/apachectl.1 start: httpd started
done.
```

See Also `switchshutdown`
`switchstart`

switchshow

Display switch and port status.

Syntax `switchshow`

Availability All users

Description Use this command to display switch and port status information. Information may vary by switch model. Below is the information provided. The first section provides switch summary information; it is followed by a section covering summary information by port.

Switch summary information:

switchName	Displays the switch symbolic name.
switchType	Displays the switch model number.

9 = DS-16B2

10.1 = ED-12000B

12.1 = DS-32B2

16.2 = DS-8B2

switchState	Displays the switch state: online, offline, testing, faulty.
switchRole	Displays the switch role: principal, subordinate, disabled.
switchDomain	Displays the switch domain ID: 0-31 or 1-239.
switchId	Displays the switch embedded port D_ID.
switchWwn	Displays the switch Worldwide Name.
switchBeacon	Displays the switch's beaconing state (either ON or OFF).
blade_n:Beacon	Displays the blade's beaconing state (either ON or OFF). Each blade is numbered by its position in the ED-12000B chassis (from 1 to 10).

The switch summary is followed by one line per port:

Area	Each slot and port combination in the ED-12000B is assigned an area number. For example, the area number of slot 3/port 15 is 63 (in switch 0), the area number for slot 10/port 15 is also 63 (in switch 1).
Slot	Slot number. The ED-12000B has 10 slots numbered from 1 to 4 and 7 to 10. Slots 5 and 6 are control processor cards.
Port	Port number. Valid values vary depending on the switch type. The ED-12000B has 16 ports per slot, and ports are numbered from 0 to 15.
SFP	Port module type (SFP or other): -- no module present sw - shortwave laser lw - longwave laser cu - copper id - serial ID
Speed	The speed of the port:

1G - 1 Gbit/sec fixed transfer speed
2G - 2 Gbit/sec fixed transfer speed
N1 - 1 Gbit/sec negotiated transfer speed
N2 - 2 Gbit/sec negotiated transfer speed
AN - Auto negotiating

State — Port state information:

No_Card - no interface card present
No_Module - no module (SFP or other) present
No_Light - module not receiving light
No_Sync - module receiving light but out of sync
In_Sync - module receiving light and in sync
Laser_Flt - module signaling a laser fault
Port_Flt - port marked faulty
Diag_Flt - port failed diagnostics
Lock_Ref - locking to the reference signal
Testing - running diagnostics
Online - port is up and running

comment — The comment field may be blank, or it may display:

Disabled - port is disabled

Bypassed - port is bypassed (loop only)

Loopback - port is in loopback mode

E_port - fabric port, shows WWN and name of attached switch

F_port - point-to-point port, shows WWN of attached N_port

G_port - point-to-point but not yet E_port or F_port

L_port - loop port, shows number of NL_ports

(Trunk master) - This port is the master port in a group of trunking ports

(Trunk port, master is port #x) - This port is configured as a trunking port, the master port is port number x.

(upstream) - This E-port is an upstream path towards the principal switch of the fabric.

(downstream) - This E-port is a downstream path away from the principal switch of the fabric.

WWN - This is the WWN of the switch connected to the E-port.

`"switch_name"` - This is the switch name of the connected switch.

Operands None

Example The following example shows a ED-12000B:

```
switch:admin> switchshow
switchName:     switch
switchType:     10.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   4
switchId:       fffc04
switchWwn:      10:00:00:60:69:00:54:e9
switchBeacon:   OFF
blade7 Beacon:  OFF
blade9 Beacon:  OFF

Area Slot Port Gbic Speed State
=====================================
  0    7    0   --    N2   No_Module
  1    7    1   --    N2   No_Module
  2    7    2   --    N2   No_Module
  3    7    3   id    N2   No_Light
  4    7    4   id    N2   Online    E-Port  (Trunk port, master is Slot  7 Port
   5)
  5    7    5   id    N2   Online    E-Port  10:00:00:60:69:00:54:e8 "san94" (up
stream) (Trunk master)
  6    7    6   id    N2   Online    E-Port  (Trunk port, master is Slot  7 Port
   5)
  7    7    7   id    N2   Online    E-Port  (Trunk port, master is Slot  7 Port
   5)
  8    7    8   --    N2   No_Module
  9    7    9   --    N2   No_Module
 10    7   10   --    N2   No_Module
 11    7   11   --    N2   No_Module
 12    7   12   id    N2   No_Light
 13    7   13   id    N2   No_Light
 14    7   14   id    N2   No_Light
 15    7   15   id    N2   Online    L-Port  8 public
 32    9    0   --    N2   No_Module
 33    9    1   --    N2   No_Module
 34    9    2   --    N2   No_Module
 35    9    3   --    N2   No_Module
 36    9    4   --    N2   No_Module
 37    9    5   --    N2   No_Module
 38    9    6   --    N2   No_Module
 39    9    7   --    N2   No_Module
 40    9    8   id    N2   Online    E-Port  (Trunk port, master is Slot  9 Port
   9)
 41    9    9   id    N2   Online    E-Port  10:00:00:60:69:50:08:d5 "sqad11" (d
ownstream) (Trunk master)
 42    9   10   id    N2   Online    E-Port  (Trunk port, master is Slot  9 Port
   9)
 43    9   11   id    N2   Online    E-Port  (Trunk port, master is Slot  9 Port
   9)
 44    9   12   --    N2   No_Module
 45    9   13   --    N2   No_Module
 46    9   14   --    N2   No_Module
 47    9   15   id    N2   Online    F-Port  10:00:00:00:c9:27:2e:9b
```

See Also switchdisable
switchenable
switchname

switchshutdown

Halt the operational switch.

Syntax `switchshutdown`

Availability Admin

Description Use this command to halt the switch operation without disrupting the other switch in the chassis. This command disables a logical switch in a ED-12000B without disturbing the software state of the system in general.

This command has to be used in combination with `switchstart`.

This command will bring down all the daemons associated with the switch; free the resources and object states associated with the switch to a clear state and will disable all the ports/blades associated with the switch.

This command is not supported on non-blade systems.

Operands None

Example **To bring down the current logical switch without disrupting the other switch in the chassis:**

```
switch:admin> switchshutdown
Stopping all switch daemons...Done.
Powering off slot 1...Done.
Powering off slot 4...Done.
Checking all slots are powered off...Done.
Cleaning up kernel modules...Done.
```

See Also `switchstart`
`switchreboot`

switchstart

Initialize the switch to operational.

Syntax `switchstart`

Availability Admin

Description This command initializes the switch without disrupting the other switch in the chassis. This command enables a logical switch in a ED-12000B without disturbing the software state of the system in general.

This command has to be used in combination with `switchshutdown`.

This command will start all the daemons associated with the switch; initialize the object states associated with the switch to a clear state and will enable all the ports/blades associated with the switch.

This command is not supported on non-blade systems.

Operands None

Example **To initialize the logical switch to operational:**

```
switch:admin> switchstart
Initializing kernel modules...Done.
Starting all switch daemons...Done.
Powering on slot 1...Done.q> to stop
Powering on slot 4...Done.q> to stop
Checking diagnostics...Done.
setup FCIP IP: ifconfig fc0 ip=0.0.0.0, netmask=255.255.255.0
```

See Also `switchshutdown`
`switchreboot`

switchstatuspolicyset

Set the policy parameters that determine the overall switch status.

Syntax `switchstatuspolicyset`

Availability Admin

Description Use this command to set the policy parameters for calculating the overall status of the switch enclosure. The policy parameter values determine how many failed or faulty units of each contributor are allowed before triggering a status change in the switch from HEALTHY to MARGINAL or DOWN.

The command will print the current parameters in a three column table format. The first column specifies the contributor; the second column specifies the minimum number that contributes to the DOWN/FAILED status; the third column specifies the minimum number that contributes to the MARGINAL/WARNING status. This command then prompts the user to change the values for each policy parameter. The default values for the policy parameters are shown in Table 1-14:

Table 1-14 Contributor Value and Status

Contributor	Default Value for DOWN	Default Value for MARGINAL
FaultyPorts	2	1
MissingSFPs	0	0
PowerSupplies	2 in the DS-32B2 3 in the ED-12000B	1
Temperatures	2	1
Fans	2	1
PortStatus	0	0
ISLStatus	2	1

Any single contributor can force the overall status of the switch to MARGINAL or DOWN. For example, assuming that the switch contributor values are set to the default values, if there is 1 faulty port

in a switch, then this contributor would set the overall switch status to MARGINAL. If 2 ports were faulty, then this contributor would set the overall switch status to DOWN.

This command enables you to set a threshold for each contributor, so that a certain number of failures are required to change the overall status of the switch.

If the value of a policy parameter is set to 0, it means that this factor is not used to determine the status of the switch. If the range of values for a particular contributor are set to 0 for both MARGINAL and DOWN, that contributor is not used in the calculation of the overall switch status.

ISLStatus monitors ISLs that are part of a defined switch group. The status of other ISLs on the same switch but outside of the group definition will not be considered when calculating switch status. If no switch groups are defined on this switch, then these ISLStatus settings will have no effect on switch status.

The ISLStatus does not affect the status of the switch as quickly as the other contributors. It may take a few minutes for a switch group ISL status change to affect the state of the switch.

When `PortStatus` monitoring is set to values of (0,0), port status changes are not logged to the event log and console. Similarly, SFP removal does not generate a message to the event log and console if `MissingSFPs` is set to (0,0). By configuring these options, the user can more closely monitor for port status and/or removal of SFPs.

Operands None

Example To change the number of FaultyPorts that define Down and Marginal:

```
switch:admin> switchstatuspolicyset

To change the overall switch status policy parameters

The current overall switch status policy parameters:
                    Down    Marginal
 ---------------------------------
       FaultyPorts  2          1
       MissingSFPs  0          0
     PowerSupplies  2          1
      Temperatures  2          1
              Fans  2          1
        PortStatus  0          0
         ISLStatus  0          0

Note that the value, 0, for a parameter, means that it is
NOT used in the calculation.
** In addition, if the range of settable values in the prompt is (0..0),
** the policy parameter is NOT applicable to the switch.
** Simply hit the Return key.

The minimum number of
  FaultyPorts contributing to
                        DOWN status: (0..32) [2] 3
  FaultyPorts contributing to
                        MARGINAL status: (0..32) [1] 2
  MissingSFPs contributing to
                        DOWN status: (0..32) [0]
  MissingSFPs contributing to
                        MARGINAL status: (0..32) [0]
  Bad PowerSupplies contributing to
                        DOWN status: (0..2) [2]
  Bad PowerSupplies contributing to
                        MARGINAL status: (0..2) [1]
  Bad Temperatures contributing to
                        DOWN status: (0..5) [2]
  Bad Temperatures contributing to
                        MARGINAL status: (0..5) [1]
  Bad Fans contributing to
                        DOWN status: (0..6) [2]
  Bad Fans contributing to
                        MARGINAL status: (0..6) [1]
  Down PortStatus contributing to
                        DOWN status: (0..32) [0]
  Down PortStatus contributing to
                        MARGINAL status: (0..32) [0]
  down ISLStatus contributing to
                        DOWN status: (0..32) [0]
  down ISLStatus contributing to
                        MARGINAL status: (0..32) [0]

Policy parameter set has been changed
   switch:admin>
```

See Also switchstatuspolicyshow
switchstatusshow

switchstatuspolicyshow

Display the policy parameters that determine the overall switch status.

Syntax `switchstatuspolicyshow`

Availability All users

Description Use this command to view the current policy parameters set for the switch. These policy parameters determine the number of failed or non-operational units allowed for each contributor before triggering a status change in the switch.

The command will print the current parameters in a three column table format. The first column specifies the contributor; the second column specifies the minimum number that contributes to the DOWN/FAILED status; the third column specifies the minimum number that contributes to the MARGINAL/WARNING status. The default values for the policy parameters are shown in Table 1-15:

Table 1-15 Contributor Value and Status

Contributor	Default Value for DOWN	Default Value for MARGINAL
FaultyPorts	2	1
MissingSFPs	0	0
PowerSupplies	2 in the DS-32B2 3 in the ED-12000B	1
Temperatures	2	1
Fans	2	1
PortStatus	0	0
ISLStatus	2	1

The policy parameters determine the number of failed or non-operational units for each contributor that trigger a status change in the switch. For example, if the FaultyPorts DOWN parameter is set to 3, and 3 ports fail in the switch, then the status of the switch changes to DOWN.

Operands None.

Example **To display the switch status policy:**

```
switch:admin> switchstatuspolicyshow
The current overall switch status policy parameters:
                    Down    Marginal
 ---------------------------------
       FaultyPorts  2         1
       MissingSFPs  0         0
     PowerSupplies  2         1
      Temperatures  2         1
              Fans  2         1
        PortStatus  0         0
         ISLStatus  0         0
```

See Also `switchstatusshow`
`switchstatuspolicyset`

switchstatusshow

Display the overall status of the switch.

Syntax `switchstatusshow`

Availability All users

Description Use this command to display the overall status of the switch. The overall status is calculated based on the most severe status of all contributors:

- Internal Switch Status
- Faulty Ports
- Missing SFPs
- Power Supplies
- Fans
- Temperatures
- Port Status

The overall status can be one of the following:

- Healthy/OK - every contributor is healthy
- Marginal/Warning - one or more components are causing a warning status
- Down/Failed - one or more contributors have failed

If the overall status is not HEALTHY/OK, the contributing factors are listed.

Operands None

Example There are two examples below. The first shows a switch with a status of MARGINAL, the second shows the same switch after all the errors have been fixed.

```
switch:admin> switchstatusshow
The overall switch status is Marginal/Warning
Contributing factors:
*  1 missing power supply triggered the Marginal/Warning status
*  1 bad fans, 2 good fans triggered the Marginal/Warning status
*  1 missing SFP triggered the Marginal/Warning status

switch:admin> switchstatusshow
The overall switch status is HEALTHY/OK
```

See Also
```
switchstatuspolicyshow
switchstatuspolicyset
```

switchuptime

Display the amount of time the switch has been operating.

Syntax `switchuptime`

Availability All users

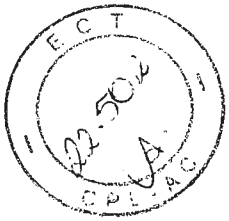
Description Use this command to display the current time and the amount of time the switch has been operational.

Operands None

Example **To view the uptime for the switch:**

```
switch:admin> switchuptime
2:00pm   up for 17 hrs 44 mins
switch:admin>
```

See Also
```
switchstart
switchshutdown
switchreboot
```



syslogdipadd

Add the IP address of a syslog daemon.

Syntax `syslogdipadd` *ip_address*

Availability Admin

Description Use this command to add the IP address of a syslog daemon, that is, the IP address of the server which is running the syslogd process. Syslog daemon (syslogd) is a process available on most UNIX systems that reads and forwards system messages to the appropriate log files and/or users, depending on the system configuration.

When one or more IP addresses are configured, the switch forwards all error log entries to the `syslogd` on the specified server(s). Up to six servers are supported.

Operands This command has the following operand:

ip_address	Specify the IP address of the server running `syslogd`. This operand is required.

Example **To add the address 192.168.1.60 to the list of machines to which system messages are sent:**

```
switch:admin> syslogdipadd 192.168.1.60
```

See Also

```
errshow
syslogdipremove
syslogdipshow
```

syslogdipremove

Remove the IP address of a syslog daemon.

Syntax `syslogdipremove` *ip_address*

Availability Admin

Description Use this command to remove the IP address of a syslog daemon, that is, the IP address of the server which is running the syslogd process.

Operands This command has the following operand:

ip_address Specify the IP address of the server running `syslogd`. This operand is required.

Example **To remove the address 192.168.1.60 from the list of machines to which system messages are sent:**

```
switch:admin> syslogdipremove 192.168.1.60
```

See Also

```
errshow
syslogdipadd
syslogdipshow
```

syslogdipshow

Display all syslog daemon IP addresses.

Syntax `syslogdipshow`

Availability All users

Description Use this command to display all syslog daemon IP addresses in the configuration database.

Operands None

Example **To display all syslog daemon IP addresses:**

```
switch:admin> syslogdipshow
syslog.IP.address.1:    192.168.1.60
syslog.IP.address.2:    192.168.1.88
syslog.IP.address.3:    192.168.2.77
```

See Also

```
errshow
syslogdipadd
syslogdipremove
```

systemtest

Run a series of diagnostic tests on a switch blade.

Syntax `systemtest [[--slot] number][-log logfile]`

Availability Admin

Description This command will run a suite of diagnostic tests on the specified switch blade. It is not required to install loop-back plugs on every port as in the case of `bladediag` and `bladediagshort`.

This command is provided just for compatibility and may be removed in the future releases.

Options This command has the following options:

`[--slot] number`	Specify which slot to operate on. If this option is not specified, the current slot will be assumed.
`-log logfile`	Indicates that the output of the command will be placed in a file named by the logfile argument. The log file will contain all activity that occurred during the execution of the command. All error messages are also saved in the logfile. If this option is not specified, no log file is created.

Examples **To run a series of diagnostic tests on a switch blade.**

```
switch:admin> systemtest --slot 1
Testing slot: 1, user ports: 3 2 1 0 7 6 5 ......
portregtest
Running portregtest ....
passed.
Test Complete: "portregtest" Pass 1 of 1
Duration 0 hr, 2 min & 14 sec (0:2:14:65).
passed.
Test return status: 0
centralmemorytest
Running centralmemorytest ............ passed.
Test Complete: "centralmemorytest" Pass 1 of 1
Duration 0 hr, 0 min & 18 sec (0:0:18:437).
passed.
Test return status: 0
<output truncated>
```

See Also `bladediag`
`bladediagshort`

systemverification

Run a suit of diagnostic tests on all switches in a fabric.

Syntax `systemverification [-parameters | -short]`

Availability Admin

Description Use this command to run a comprehensive system wide test of all switches in a fabric. It will initiate a burnin run on all switches within the current system.

The run can be terminated by issuing a CTRL-C character from the initiating terminal. All of the burnin features are operational during the `systemverification` command. The `burninerrshow` will display the stored burnin errlogs, the logs by blade are saved in `/var/log/switchburnin.<switch>.<slot>` files. On the fixed port count products, the slot defaults to 0.

The command monitors the testing, and will terminate the burnin activity if all the elements have failed. Each failing slot will only output the first observed fail. Since this monitoring is a polling activity, the command number output may not be the exact command number that failed. After the testing has terminated, `burninstatus` command is output, and the `burninerrshow` messages for the failing slots are output. If all slots pass, then only the `burninstatus` command output is displayed.

The burnin tests are designed to operate with switches connected to a fabric and restricts the frame loopback to inside the unit. If loopback plugs are installed in all ports, the burnin parameter min_lb_mode can be changes to 1 to test the fibre channel through the loopback plug.

Options This command has the following options:

-parameters Invokes the `diagsetcycle` command before starting the burnin run. This will allow users to modify the burnin parameters prior to the run. These `diagsetcycle` parameters are copied to all switches in the system and override the original settings in the database. If the `diagsetcycle` parameter is not

specified, then the run will use the previously stored values. This option does not performs a `burninerrclear` operation prior to starting the testing operation.

-short Sets the burnin parameters that control the number of frames to 1. The primary use for this command is for software regression testing, or a quick validation that all hardware is operational. The shorter test cycle will not have enough test time to detect intermittent errors. This option performs a `burninerrclear` operation prior to starting the testing operation.

Errors Each diagnostic test in this suit may report its own set of error messages when it detects failure(s). Refer to the *Errors* section of the individual commands. These messages are only available in the log file.

Example To initiate a system verification test on all switches in the fabric:

```
switch:admin> systemverification -short
     systemverification: Setting parameters for short run.
     systemverification: burnin parameters.
     CURRENT - KEYWORD        : DEFAULT
1      - number_of_runs         : 1
      2       - vib    : 2
      10      - thermal        : 10
      SYSTEMVERIFICATION      - label : BURNIN
      2       - min_lb_mode    : 2
      1       - tbr_passes     : 1
      1       - prt_on         : 1
      1       - cntmem_on      : 1
      1       - cmi_on         : 1
      1       - retention_on   : 1
      1       - cam_on         : 1
      1       - flt_passes     : 50
      1       - sta_passes     : 25
      1       - plb_nframes    : 100
      1       - txd_nframes    : 50
      1       - xpt_nframes    : 200
      1       - bpt_nframes    : 20
      1       - slk_nmegs      : 50
      1       - bpt_all_nframes        : 30
      1       - slk_all_nmegs : 50
     systemverification: Arming the burnin run on switch 0.
     systemverification: Starting burnin on Switch 0
     systemverification: Monitoring progress of the burnin activity.
     systemverification: Outputting Status
     State           Status  Run     Cmd     TotCmds Script
     COMPLETED       PASS    1       22      22      switchburnin.sh
```

See Also `diagsetcycle`
`diagsetburnin`
`burninstatus`
`burninerrclear`

tempshow

Display temperature readings.

Syntax `tempshow`

Availability All users

Description Use this command to display the current temperature readings of all temperature sensors in a switch. Each temperature sensor has an

index. The indices start from 1. There can be more than one sensor per slot. The slot number to which a sensor belongs is displayed in the column next to the index. The temperature readings are given in both Centigrade and Fahrenheit.

Refer to the Hardware Reference Manual for your switch to determine the normal temperature range values.

Operands None

Example This example shows a ED-12000B:

```
switch:admin> tempshow

Index   Slot    State           Centigrade      Fahrenheit
=========================================================
1       1       Ok                47              116
2       2       Absent
3       3       Absent
4       4       Ok                46              114
5       5       Ok                33               91
6       6       Ok                33               91

   switch:admin>
```

For the ED-12000B, this command only returns the temperature sensor values for the logical switch you are logged into, not for the entire chassis.

This example shows a DS-32B2:

```
switch:admin> tempshow

Index   Slot    State           Centigrade      Fahrenheit
=========================================================
  1       0       Ok                39              102
  2       0       Ok                41              105
  3       0       Ok                27               80
  4       0       Ok                39              102
  5       0       Ok                42              107

switch:admin>
```

See Also `sensorshow`
`fanshow`
`psshow`
`slotshow`

timeout

Set or show the IDLE timeout value for a login session.

Syntax `timeout [timeval]`

Availability Admin (show / set)

All users (for viewing only)

Description Use this command with no operands to display the current telnet timeout value. Use this command with an operand to sets the idle timeout value to the specified minutes. Using a timeout value of zero will disable the timeout functionality so that login sessions would never be disconnected.

Operands This command has the following operand:

timeval	Specify the number of minutes for the telnet timeout value. This operand is optional.

Example **To set the idle timeout to 10 minutes:**

```
switch:admin> timeout 10
IDLE Timeout Changed to 10 minutes
The modified IDLE Timeout will be in effect after NEXT login
switch:admin>
```

topologyshow

Display the unicast fabric topology.

Syntax `topologyshow [domainnumber]`

Availability All users

Description Use this command to display the fabric topology, as it appears to the local switch.

This includes:

- A list of all domains that are part of the fabric, and to each of those domains, all possible paths from the local switch.

- For each path - cost, the number of hops from the local switch to the destination switch, and a summary of all ports are routed through that path.

A path is described by the output port that a frame addressed to a certain domain will be forwarded to by the switches' routing hardware, in order to reach the domain.

With the domain number specified, this command displays the topology information for the specified destination domain.

The display contains the following fields:

Local Domain ID	Domain number of local switch.
Domain	Domain number of destination switch.
Metric	Cost of reaching destination domain.
Name	The name of the destination switch.
Path Count	The number of currently active paths to the destination domain.
Hops	The maximum number of hops to reach destination domain.
Out Port	Port that incoming frame will be forwarded to, in order to reach the destination domain.
In Ports	Input ports that use the corresponding Out Port to reach the destination domain. This is the same information provided by `portrouteshow` and `urouteshow`.
Total Bandwidth	The maximum bandwidth of the out port.
Bandwidth Demand	The maximum bandwidth demand by the in ports.
Flags	Always 'D', indicating a dynamic path. A dynamic path is discovered automatically by the FSPF path selection protocol.

Operands This command has the following operand:

domainnumber Specify the destination domain for which topology information is to be displayed. This operand is optional. When no domain number is specified, this command displays the topology information of all the domains in the fabric.

Examples

To display the unicast fabric topology:

```
switch:admin> topologyshow

2 domains in the fabric; Local Domain ID: 1
Domain:          6
Metric:          500
Name:            switch
Path Count:      4
        Hops:                   1
        Out Port:               60
        In Ports:               None
        Total Bandwidth:        2 Gbps
        Bandwidth Demand:       0 %
        Flags:                  D

        Hops:                   1
        Out Port:               61
        In Ports:               None
        Total Bandwidth:        2 Gbps
        Bandwidth Demand:       0 %
        Flags:                  D

        Hops:                   1
        Out Port:               62
        In Ports:               None
        Total Bandwidth:        2 Gbps
        Bandwidth Demand:       0 %
        Flags:                  D

        Hops:                   1
        Out Port:               58
        In Ports:               None
        Total Bandwidth:        2 Gbps
        Bandwidth Demand:       0 %
        Flags:                  D
```

See Also

portrouteshow

urouteshow

trackchangeshelp

Display information on track-changes feature commands.

Syntax `trackchangeshelp`

Availability All users

Description Use this command to display information about the track-changes commands.

Example **To display information on the track-changes feature commands:**

```
switch:admin> trackchangeshelp
trackChangesSet    Configure alert for login/logout/config update
trackChangesShow   Displays status of track changes
```

See Also
`trackchangesset`
`trackchangesshow`

trackchangesset

Enable configuring of track-changes feature.

Syntax `trackchangesset [mode] [, snmptrapmode]`

Availability Admin

Description This command enables or disables the track-changes feature. An SNMP-TRAP mode can also be enabled. Trackable changes are:

- Successful login
- Unsuccessful login
- Logout
- Config file change from task
- Track-changes on
- Track-changes off

The output from the track-changes feature is dumped to the error log for the switch. Use the `errdump` command or `errshow` command to view the error log.

Operands This command has the following operands:

mode	Specify 1 to enable the track-changes feature or specify 0 to disable the feature. The default (if no operand is specified) is to disable the track-changes feature. This operand is optional.
snmptrapmode	Specify 1 to enable errors to be sent to the SNMP-TRAP in addition to the errlog or specify 0 to disable the SNMP-TRAP messages. The default (if no operand is specified) is to disable SNMP-TRAP messages. This operand is optional.

Example **To enable the Track Changes feature:**

```
switch:admin> trackchangesset 1, 1
Committing configuration...done.
switch:admin> trackchangesshow
Track changes status: ON
Track changes generate SNMP-TRAP: YES
switch:admin>
```

See Also

```
agtcfgset
agtcfgshow
trackchangesshow
trackchangeshelp
```

trackchangesshow

Display status of track-changes feature.

Syntax `trackchangesshow`

Availability All users

Description Use this command to display status of the track-changes feature. It shows if the feature is turned on or off and if SNMP traps are generated.

The output from the track-changes feature is dumped to the error log for the switch. Use the `errdump` command or `errshow` command to view the error log.

Operands None

Example **To display the status of the track-changes feature:**

```
switch:admin> trackchangesshow
```

```
Track changes status: ON
Track changes generate SNMP-TRAP: YES
```

See Also

```
trackchangesset
trackchangeshelp
```

trunkdebug

Debug a trunk link failure.

Syntax `trunkdebug port1, port2`

Availability Admin

Description Use this command to debug a trunk link failure. This command reports one of the following messages based on the trunking properties of the two specified ports:

- Switch does not support trunking
- Trunking license required
- port<port_id> is not E_port
- port<port_id> trunking disabled
- port<port_id> speed is not 2G
- port<port_id> and port<port_id> are not on same quad
- port<port_id> and port<port_id> connect to different switches
- port<port_id> is not Trunking port due to: E_port being disabled, or trunking may be disabled at remote port
- port<port_id> and port<port_id> can't trunk, please check link length to make sure difference is less than 400 m

Operands This command has the following operands:

port1	Specify the area number of port1. Use the `switchshow` command to view the area numbers for a port. This operand is required.
port2	Specify the area number of port2. Use the `switchshow` command to view the area numbers for a port. This operand is required.

Example **To debug a trunk connection:**

```
switch:admin> trunkdebug 3, 4
```

```
port 3 is not E port
```

See Also

```
trunkshow
portcfgtrunkport
switchcfgtrunk
```

trunkshow

Display trunking information.

Syntax

```
trunkshow
```

Availability

All users

Description

Use this command to display trunking information. The fields displayed are as follows:

Trunking Group Number
: Displays each trunking group on a switch. All the ports that are part of this trunking group are displayed.

Port to port connections
: Displays the port-to-port trunking connections.

WWN
: Displays the WWN of the connected port.

deskew
: The time difference for traffic to travel over each ISL as compared to the shortest ISL in the group. The number corresponds to nanoseconds divided by 10. The firmware automatically sets the minimum deskew value of the shortest ISL to 15.

Master
: Displays whether this trunking port connection is the master port connection for the trunking group.

Operands

None

Example To display trunking information for a switch:

```
switch:admin> trunkshow

 1: 2 -> 60   10:00:00:60:69:80:4f:85   deskew 16   MASTER
    3 -> 61   10:00:00:60:69:80:4f:85   deskew 15

 2: 7 -> 39   10:00:00:60:69:80:4f:85   deskew 17   MASTER
    6 -> 38   10:00:00:60:69:80:4f:85   deskew 16
    5 -> 36   10:00:00:60:69:80:4f:85   deskew 16
    4 -> 37   10:00:00:60:69:80:4f:85   deskew 15

 3:24 -> 56   10:00:00:60:69:80:4f:85   deskew 16   MASTER
   25 -> 57   10:00:00:60:69:80:4f:85   deskew 15

 4:29 -> 33   10:00:00:60:69:80:4f:85   deskew 16   MASTER
   28 -> 32   10:00:00:60:69:80:4f:85   deskew 15

switch:admin>
```

See Also `portcfgtrunkport`
`switchcfgtrunk`

tsclockserver

Display or set the NTP Server address.

Syntax `tsclockserver [ipaddr]`

Availability All users (display)

Admin (set)

Description Use this command to synchronize the local time of the Principal or Primary FCS switch to an external NTP server.

The Time Server daemon synchronizes fabric time by sending updates of the Principal or Primary FCS local switch time periodically to every switch in the fabric. The Time Server daemon runs on all switches in the fabric, but only the Principal switch (when the Security feature not enabled), or the Primary FCS switch (when the Security feature is enabled) connect to the NTP server, and broadcast Time Service updates.

All switches in the fabric maintain the current clock server IP address in non-volatile memory. By default this value is LOCL. Changes to the

clock server IP address on the Principal or Primary FCS switch are propagated to all switches in the fabric.

Use this command with no parameters to display the current clock server IP address being used. Specify the *ipaddr* operand to set the clock server IP address, and enable fabric wide clock synchronization with the specified clock server.

The NTP server used MUST support a full NTP client. Fabric OS v3.1 and v2.6.1 have an SNTP client and hence will accept an SNTP or NTP server but v4.1 has an NTP client; So for the proper functioning of a mixed fabric with external time synchronization it is necessary that an NTP server that supports a full NTP client be used.

The *ipaddr* specified should be the IP address of an NTP server and should be accessible from the switch. When a clock server IP address other than LOCL is specified but is not used by the fabric, a warning is displayed and logged. When a clock server IP address other than LOCL is specified, the `date` command will be restricted to display only. See the `date` command for more details.

When secure mode is enabled, this command can be run on all switches to view the NTP server's IP address. You can only modify the the NTP server's IP address on the Primary FCS switch.

Operands

This command has the following operand:

ipaddr	Specify the IP address of the NTP server. This operand is optional. By default this value is LOCL.

If no operand is specified the current value is displayed.

Example

The following example shows how to display the current clock server value (LOCL), set the value to an NTP server at the specified IP address, and then verify that the new IP address was saved.

```
switch:admin> tsclockserver
LOCL
switch:admin> tsclockserver "123.123.123.123"
Updating Clock Server configuration...done.
switch:admin> tsclockserver
123.123.123.123
switch:admin>
```

See Also

`date`

tshelp

Display the time service commands.

Syntax `tshelp`

Availability All users

Description Use this command to display a list of time service commands.

Example **To display a list of time service commands:**

```
switch:admin> tshelp

tsTimeZone              Display or set the system Time Zone
tsClockServer           Display or set the NTP Server address
switch:admin>
```

tstimezone

Display or set the system time zone.

Syntax `tstimezone [houroffset [, minuteoffset]]`

Availability All users (display)

Admin (set)

Description Use this command to display or set the system time zone.

All switches maintain the current time zone setup in non-volatile memory. Changing the Time Zone on a switch updates the local time zone setup and is reflected in local time calculations.

All switches are by default in the 0,0 time zone, that is GMT. If all switches in a fabric are in one time zone, it is possible to leave the time zone setup at the default.

Time zone is used only in computing local time which is used for error reporting and logging. An incorrect time zone setup will not affect the switch operation in any way.

Enter this command with no parameters, to display the time zone setup. With the valid parameters, it sets the time zone for an individual switch.

Negative *houroffset* values mean the local time is behind GMT.

Example: -8,0 is GMT-08:00

Positive *houroffset* values mean the local time is ahead of GMT.

Example: 3, 0 is GMT+03:00

Operands This command has the following operands:

houroffset	Specify the number of hours relative to GMT. This operand must be specified as an integer. Valid values are -12 through 12. This operand is optional.
minuteoffset	Specify the number of minutes relative to the hourOffset. This operand must be specified as an integer. Valid values are -30, 0, or 30. This operand is optional.

Examples **To display the current time zone setup, then changes them to GMT-3:30:**

```
switch:admin> tstimezone
Time Zone Hour Offset: 0
Time Zone Minute Offset: 0
switch:admin> tstimezone -3, -30
Updating Time Zone configuration...done.
switch:admin> tstimezone
Time Zone Hour Offset: -3
Time Zone Minute Offset: -30
```

See Also `date`

turboramtest

Turbo SRAM logic test for 2 Gbit/sec ASICs.

Syntax `turboramtest [--slot number] [-passcnt count] [-ports itemlist]`

Availability Admin

Description This command verifies the on chip SRAM located in the 2 Gbit/sec ASIC using the Turbo-Ram BIST circuitry. These same SRAMS are tested by `portregtest` and `sramretentiontest` using PCI operations, but for this test the BIST controller is able to perform the SRAM write and read operations at a much faster rate. It is also able to test one SRAM in each quadrant of every chip in parallel.

The test flow for each SRAM is as follows:

1. Fill RAM with alternating FFFF 0000 pattern. (Subtest 1: turboram memory fill)
2. For each incrementing address read FFFF 0000 pattern and write 0000 FFFF. (Subtest 2: turbo-ram r-m-w inc 1)
3. For each incrementing address read 0000 FFFF pattern and write FFFF 0000. (Subtest 3: turbo-ram r-m-w inc 2)
4. For each decrementing address read FFFF 0000 pattern and write 0000 FFFF. (Subtest 4: turbo-ram r-m-w dec 1)
5. For each decrementing address read 0000 FFFF pattern and write FFFF 0000. (Subtest 5: turbo-ram r-m-w dec 2)
6. Repeat steps 1-5 with AAAA 5555 pattern.

Operands This command has the following operands:

`--slot` *number* Specify the slot number in a ED-12000B switch. The slot number must be followed by a slash (/) and the port number.

The ED-12000B has a total of 10 slots counted from 1 to 10. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are switch cards. On each switch card, there are 16 ports counted from the bottom 0 to 15. A particular port must be represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

This operand is not required for switches that do not have slots.

`-passcnt` *count* Specify the number of times to perform this test. The default value is 1. This operand is optional.

`-ports` *itemlist* Specify a list of blade ports to test. By default all the blade ports in the specified slot are tested. Refer to the `itemlist` command help page for more information. This operand is optional.

Example To execute this test:

```
switch:admin> turboramtest -passcnt 2 -ports 2/0-2/63
Running Turbo RAM Test ........ passed.
```

Errors When it detects failure(s), the subtest may report one or more of the following error messages:

```
DIAG-WTEST
DIAG-INC_RWTEST
DIAG-DEC_RWTEST
DIAG-RAMINIT_TO
```

See Also

```
portregtest
centralmemorytest
cmitest
camtest
sramretentiontest
```

txdpath

Functional test of ASIC pair TXA, TXD connections.

Syntax `txdpath [--slot` *number*`] [-nframes` *count*`] [-lb_mode` *mode*`] [-spd_mode` *mode*`] [-nonstop` *mode*`] [-ports` *itemlist*`]`

Availability Admin

Description Use this command to verify the TXA, TXD, and CMI data paths between the chips within a mini-switch. This is done by configuring all of the ports on the mini-switch in internal loopback and sending a frame from each quadrant to each other port on the same mini-switch. The frame starts from the CPU and is transmitted by the first port which also receives the frame and deposits it in central memory. The second port then reads the frame from central memory using it's own TXA,TXD path. The frame is then looped back one more time and is sent back to the CPU where it is compared with the transmitted data.

Only one frame is transmitted and received at any one time. External cable is not required to run this test. The port LEDs flicker green rapidly while the test is running. The test method is as follows:

1. Set all ports present for parallel loopback. Then for each pair of source quadrants and destination ports:

2. Set up source port to route frames to destination port and destination port to route frames to CPU.
3. Transmit frame F via source port.
4. Pick up the frame from destination port.
5. Check if any of the 8 statistic error counters are non-zero:

   `ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF, Enc_out, BadOrdSet, DiscC3.`

6. Repeat steps 2 through 5 for all ports present until:
   - The number of frames (or `-nmegs` *`count`*) requested is reached,
   - All ports are marked bad.

At each pass, a different data type is used to create the frame from a palette of 7; meaning if a pass of 7 is requested, 7 different frames are used in the test. If 8 passes, the first 7 frames are unique, and the 8th is the same as the first. The data palette of 7 are:

1. CSPAT: 0x7e, 0x7e, 0x7e, 0x7e, ...
2. BYTE_LFSR: 0x69, 0x01, 0x02, 0x05, ...
3. CHALF_SQ: 0x4a, 0x4a, 0x4a, 0x4a, ...
4. QUAD_NOT: 0x00, 0xff, 0x00, 0xff, ...
5. CQTR_SQ: 0x78, 0x78, 0x78, 0x78, ...
6. CRPAT: 0xbc, 0xbc, 0x23, 0x47, ...
7. RANDOM: 0x25, 0x7f, 0x6e, 0x9a, ...

If seven passes are requested, the seven different data types are used in the test. If eight passes are requested, the first seven frames use unique data type.

The following operands are optional.

Options This command has the following options:

`--slot` *`number`* This option specifies the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is set to 0 and designed to operate on fixed port count products.

`-nmegs` *count*

Specify the number of million frames to send. The test will progress until the specified number of frames has been transmitted on each port. The default value is 10, so the number of frames sent will be at least 10 million.

`-lb_mode` *mode*

Specify the loopback point for the test. By default, this command uses loopback plugs as described above. However for debug purposes you can select other loopback modes as follows:

0: Cable Loopback.

1: Port Loopback (loopback plugs).

2: External (SERDES) loopback.

3: Silkscreen loopback.

4: Serial link wrapback.

5: Internal (parallel) loopback.

`-spd_mode` *mode*

Specify the speed mode for the test. For 1 Gbit/sec only products it is ignored. The exact operation of modes 3 through 6 depends upon the loopback mode selected. When speed modes 3 through 6 are used with cables, they must be connected EVEN to ODD or the test will fail.

- 0: set all ports' speed for auto-negotiate.
- 1: set all ports' speed to lock at 1 Gbit/sec.
- 2: set all port's speed to lock at 2 Gbit/sec.

For `lbMode == 0,1` the following speed modes are available to test the speed negotiation:

- 3: set all even ports' speed for auto-negotiate, set all odd ports' speed for 1 Gbit/sec.
- 4: set all even ports' speed for auto-negotiate, set all odd ports' speed for 2 Gbit/sec.
- 5: set all odd ports' speed for auto-negotiate, set all even ports' speed for 1 Gbit/sec.

- 6: set all odd ports' speed for auto-negotiate, set all even ports' speed for 2 Gbit/sec.

For `lbMode== 2,3` the following speed modes are available to test fifo underrun.

- 3,5: set all even ports' speed for 2 Gbit/sec, set all odd ports' speed for 1 Gbit/sec.
- 4,6: set all even ports' speed for 1 Gbit/sec, set all odd ports' speed for 2 Gbit/sec.

`-nonstop` *mode* — Specify the non-stop mode. If set to non-zero value, test will not stop on the first error. The default value is 0.

`-ports` *itemlist* — Specify a list of user ports to test. By default all of the user ports in the current switch are tested. This option may be used to restrict testing to the specified ports.

Example

To run the txdpath test:

```
switch:admin> txdpath
Running TX Data Path Test ....
Test Complete: "txdpath" Pass 10 of 10
Duration 0 hr, 0 min & 47 sec (0:0:47:645).
```

Errors

When it detects failure(s), the test may report one or more of the following error messages:

```
DATA
ERRSTAT
INIT
PORTDIED
STATS
TIMEOUT
XMIT
```

See Also

```
backport
camtest
centralmemorytest
cmemretentiontest
cmitest
crossporttest
itemlist
portloopbacktest
portregtest
spinsilk
sramretentiontest
```

uptime

Display length of time the system has been operational.

Syntax `uptime`

Availability All users

Description Use this command to display the length of time the system has been in operation (also known as *up time*), the total cumulative amount of up time since the system was first powered-on, the date and time of the last reboot, and the reason for the last reboot.

For up and powered-on times less than 60 seconds, the time is displayed in seconds. For times greater than or equal to 60 seconds, the time is displayed in minutes. The output format adjusts accordingly.

The reason for the last switch reboot is also recorded in the error log. Reasons are listed below. Not all the below responses are applicable to all switch models:

Unknown	Reason is unknown.
Bus time-out*	Port ASIC was accessed and no response was received.
Bus error*	Non-existent system address was accessed.
Panic*	Firmware detected a critical hardware error or an internal inconsistency.
Fault*	CPU signaled a fault condition (critical firmware error).
Power-on	Last reboot was caused by a power-on.
Watchdog*	Watchdog timer caused a reset.
PushButtons	Push buttons 1 and 3 were depressed for two seconds, causing a system reset.
Reboot	Last reboot was caused by a user (from any management interface).
Powerfail NMI*	Power supply caused a nonmaskable interrupt.
Watchdog NMI*	Watchdog timer caused a nonmaskable interrupt.

PushButton NMI*	Push buttons 2 and 4 were depressed for two seconds, causing a nonmaskable interrupt.
Software NMI*	Firmware caused a nonmaskable interrupt.

The items marked with an asterisk (*) are usually caused by hardware or firmware failures. Information on the failure is stored in the switch. Follow the procedures in the switch manual.

Operands None

Example **To display the length of time the system has been operational:**

```
switch:admin> uptime
12:03am  up  4:56,  3 users,  load average: 1.17, 1.08, 1.08
```

See Also
```
date
fastboot
reboot
```

urouteconfig

Configure a static route.

Syntax `urouteconfig` *`InArea Domain OutArea`*

Availability Admin

Description Use this command to configure static routes. A static route is a route that is assigned to a specific path, and will not change when a topology change occurs, unless the path used by the route becomes unavailable.

After this command is issued, and if *`OutArea`* is a usable port, all frames coming in from InArea port addressed to *`Domain`* will be forwarded through OutArea port.

If OutArea port is not usable, then the routing assignment is not affected by this command. When OutArea port becomes usable again, the static route assignment for *`InArea`* is enforced.

OutArea port is usable if it is on a minimum cost path to the destination domain.

InArea port can be either an F_Port or an E_Port.

When using static routes, load sharing may be affected. The switch attempts to achieve optimum load sharing, but if too many routes are statically configured to use the same output port, a fair load sharing may not be achievable.

In order to prevent routing loops, static route configuration using a non-minimum cost path is not allowed. If an attempt is made to configure such a route, the user is queried on whether or not the entry should be saved in the database.

Operands This command has the following operands:

InArea	Specify the port to be statically routed. This operand is required.
Domain	Specify the destination domain. This operand is required.
OutArea	Specify the output port where traffic is forwarded. This operand is required.

Examples

To configure a static route for all traffic coming in from port 1 and addressed to domain 2 to go through port 5:

```
switch:admin> urouteconfig 1 2 5
done.
switch:admin> configshow
route.ucastRoute.1.2: 5
route.ucastRouteCount: 1
```

See Also

```
configshow
interfaceshow
urouteremove
urouteshow
```

urouteremove

Remove a static route.

Syntax `urouteremove` *InArea Domain*

Availability Admin

Description Use this command to remove a previously configured static route.

After this command is issued, the route to *Domain* for *InArea* may or may not change. It changes if the previous static route was not along a minimum cost path. Also, after this command is issued, the load sharing to *Domain* is re-evaluated.

InArea can be either an F_Port or an E_Port.

Operands This command has the following operands:

InArea	The port that is statically routed. This operand is required.
Domain	The destination domain. This operand is required.

Examples

To remove a static route for all traffic coming in from port 1 and addressed to domain 2:

```
switch:admin> urouteremove 1 2
done.
```

See Also

```
configshow
urouteconfig
urouteshow
```

urouteshow

Display unicast routing information.

Syntax `urouteshow [slotnumber/] [portnumber] [, domainnumber]`

Availability All users

Description Use this command to display the unicast routing information for a port, as it is known by the FSPF path selection and routing task. The routing information describes how a frame that is received from a port on the local switch is to be routed to reach a destination switch.

When no operand is specified, this command displays the routing information for all the active ports on the local switch, to all the domains in the fabric.

When only slot number and port number are specified, this command displays the routing information for the specified port to all the domains connected to it.

When slot number, port number, and domain number are all specified, this command only displays the routing information for the specified port to the specified domain.

The following information is displayed:

Local Domain ID: Domain number of local switch.

In Port: Port from which a frame is received.

Domain: Destination domain of incoming frame.

Out Port: Port to which the incoming frame is to be forwarded.

Metric: Cost of reaching the destination domain.

Hops: Maximum number of hops required to reach the destination domain.

Flags: Indicates if route is dynamic (D) or static (S). A dynamic route is discovered automatically by the FSPF path selection protocol. A static route is assigned using the command `urouteconfig`.

Next (Dom, Port): Domain and port number of the next hop. These are the domain number and the port number of the switch to which Out Port is connected.

The information provided by this command should match what is provided by `portrouteshow` and `topologyshow`.

Operands

This command has the following operands:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

`portnumber` Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

domainnumber Displays routing information for the specified domain. This operand is optional. This operand should only be specified when the port number is specified.

If no operand is specified, this command displays routing information for all active ports on the local switch, to all the domains in the fabric.

Examples

The first example displays the routing information of all the active ports, The second command displays the routing information of port 11 on slot 1, and the third command displays the routing information of port 11 to domain 4 only:

```
switch:admin> urouteshow
   Local Domain ID: 3
   In Port    Domain    Out Port    Metric    Hops    Flags    Next (Dom,
   Port)
   ------------------------------------------------------------------------
   ---
    0          1          11        1000       1       D           1,0
   11          2           0        1500       2       D           4,0
               4           0         500       1       D           4,0
   16          1          27        1000       1       D           1,1
   27          2          16        1500       2       D           4,16
               4           0         500       1       D           4,0

switch:admin> urouteshow 1/11
   Local Domain ID: 3
   In Port    Domain    Out Port    Metric    Hops    Flags    Next (Dom,
   Port)
   ------------------------------------------------------------------------
   ----
    11          2          16        1500       2       D           4,16
                4          16         500       1       D           4,16

switch:admin> urouteshow 1/11, 4
           Local Domain ID: 3
   In Port    Domain    Out Port    Metric    Hops    Flags    Next (Dom,
   Port)
   ------------------------------------------------------------------------
   ----
   11          4          16         500       1       D           4,16
```

See Also

portrouteshow
topologyshow
urouteconfig
urouteremove

version

Display firmware version information.

Syntax `version`

Availability All users

Description Use this command to display firmware version information and build dates.

The following is displayed:

Kernel:	Displays the version of switch kernel operating system;
Fabric OS:	Displays the version of switch Fabric OS;
Made on:	Displays the build date of firmware running in switch;
Flash:	Displays the build date of firmware stored in flash proms;
BootProm:	Displays the version of the firmware stored in the boot PROM.

Usually the Made on and Flash dates are the same, since the switch starts running flash firmware at power-on. However, in the time period between `firmwaredownload` and the next `reboot`, the dates can differ.

Operands None

Example The following example shows the firmware version information on a DS-32B2:

```
switch:admin> version
Kernel:     2.4.19
Fabric OS:  v4.1.0
Made on:    Mon Oct 7 09:27:16 2002
Flash:      Tue Oct 8 12:13:47 2002
BootProm:   3.1.18
switch:admin>
```

See Also

```
firmwaredownload
reboot
```

wwn

Display a switch WWN.

Syntax `wwn`

Availability factory or root only (set)

All users (display)

Description Use this command to modify or display the WWN of a switch. All switches have a numeric address that is the unique fibre channel address used for communicating with the switch. The wwn is shown in the output of the `switchshow` command.

This command with no parameters displays the current WWN value.

This command with a parameter sets the switch's WWN to the new value. WWN names must have eight colon separated fields each consisting of 1 or 2 hexadecimal digits between 0 and off, with no spaces.

After the world wide name is changed, the user is prompted to reboot the switch. The name will not take effect until the switch restarts.

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example **To display the switch WWN:**

```
switch:admin> wwn
10:00:00:60:69:00:54:e9

switch:admin>
```

See Also `switchshow`

zoneadd

Add a member to the zone.

Syntax `zoneadd "zoneName", "member;member"`

Availability Admin

This command requires a Zoning license.

Description Use this command to add one or more members to an existing zone.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands The following operands are required:

zoneName	Specify the name of an existing zone, in quotation marks. This operand is required.
member	Specify a member or list of members to be added, in quotation marks, separated by semi-colons. Valid values can be one or more of the following: • A switch domain and port area number pair. For example, `"2, 20"`. View the area numbers for ports using the `switchshow` command. • Node or port WWN. • QuickLoop AL_PA • Zone alias name

Example **To add aliases for three disk arrays to "Blue_zone":**

```
switch:admin> zoneadd "Blue_Zone", "array3; array4; array5"
```

See Also `zonecreate`
`zonedelete`
`zoneremove`

zoneshow

zonecreate

Create a zone.

Syntax `zonecreate "zonename", "member;member"`

Availability Admin

This command requires a Zoning license.

Description Use this command to create a new zone.

A zone name is a C-style name beginning with a letter and followed by any number of letters, digits, and underscore characters. Names are case sensitive; for example, `"Zone_1"` indicates a different zone than `"zone_1"`. Blank spaces are ignored.

The zone member list must have at least one member (empty lists are not allowed). The members are described by a list of member definitions separated by semi-colons.

Specify ports by domain and port area number. The values are entered as a pair of numbers `"s,p"` where `s` is the switch number (domain ID) and `p` is the port area number. For example, `"2, 20"` specifies port area number 20 on switch domain 2. When a zone member is specified by port area number, then all devices connected to that port are in the zone. If this port is an arbitrated loop, then all devices on the loop are in the zone.

Specify a *Worldwide Name* as eight hex numbers separated by colons, for example `10:00:00:60:69:00:00:8a`. Zoning compares the WWN with the node and port names presented by a device in a login frame (FLOGI or PLOGI). When a zone member is specified by node name, then all ports on that device are in the zone. When a zone member is specified by port name, then only that single device port is in the zone.

Specify a *QuickLoop AL_PA* as a QuickLoop name followed by a list of AL_PAs, for example `qloop1[01,02]`. QuickLoop names have the same format as zone names, and are created with the `qloopcreate` command to define a switch or pair of switches that form the QuickLoop.

Specify a zone alias name using the same format as a zone name. It is created with the `alicreate` command. The alias must resolve to a list of one or more of the following:

- A switch domain and port area number pair. View the area numbers for ports using the `switchshow` command.
- Worldwide Names
- QuickLoop AL_PAs

The types of zone members used to define a zone may be mixed. For example, a zone defined with the following members: `"2,12; 2,14; 10:00:00:60:69:00:00:8a"` would contain all devices connected to switch 2, ports 12 and 14, and to the device with the Worldwide Name `"10:00:00:60:69:00:00:8a"` (either node name or port name), at the port in the fabric to which it is connected.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

Use this command to create a *broadcast* zone. This is a special zone used to specify those nodes that can receive broadcast traffic. Broadcast traffic is usually meant for servers and not for storage devices. This zone must be named `"broadcast"`. Only one broadcast zone can exist within a fabric. This type of zone is hardware enforced; the switch controls data transfer to a port.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands

The following operands are required:

zonename — Name for a zone to be created, in quotation marks. This name cannot be used for any other zone object.

member — List of members to be included in zone, in quotation marks, separated by semi-colons. Can be one or more of the following:

- A switch domain and port area number pair. For example, `"2, 20"`. View the area numbers for ports using the `switchshow` command.
- Worldwide Names

- QuickLoop AL_PAs
- Zone alias names

Example To create three zones using a combination of port numbers and zone aliases:

```
switch:admin> zonecreate "Red_zone", "1,0; loop1"
switch:admin> zonecreate "Blue_zone", "1,1; array1; 1,2; array2"
switch:admin> zonecreate "Green_zone", "1,0; loop1; 1,2; array2"
```

See Also
```
zoneadd
zonedelete
zoneremove
zoneshow
```

zonedelete

Delete a zone.

Syntax `zonedelete "zonename"`

Availability Admin

This command requires a Zoning license.

Description Use this command to delete a zone.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

zonename	Name of the zone to be deleted, in quotation marks. This operand is required.

Example To delete the zone "Blue_zone":

```
switch:admin> zonedelete "Blue_zone"
```

See Also

```
zoneadd
zonecreate
zoneremove
zoneshow
```

zonehelp

Display help information on zone commands.

Syntax

```
zonehelp
```

Availability

All users

Description

Use this command to display help information on zone commands.

Operands

None

Example

To display zone command help information:

```
switch:admin> zonehelp

aliAdd                  Add a member to a zone alias
aliCreate               Create a zone alias
aliDelete               Delete a zone alias
aliRemove               Remove a member from a zone alias
aliShow                 Print zone alias information

cfgAdd                  Add a member to a configuration
cfgCreate               Create a zone configuration
cfgDelete               Delete a zone configuration
cfgRemove               Remove a member from a configuration
cfgShow                 Print zone configuration information

qloopAdd                Add a member to a qloop
qloopCreate             Create a qloop
qloopDelete             Delete a qloop
qloopRemove             Remove a member from a qloop
qloopShow               Print qloop information

zoneAdd                 Add a member to a zone
zoneCreate              Create a zone
zoneDelete              Delete a zone
zoneRemove              Remove a member from a zone
zoneShow                Print zone information

fazoneAdd               Add a member to a fabric assist zone
fazoneCreate            Create a fabric assist zone
fazoneDelete            Delete a fabric assist zone
fazoneRemove            Remove a member from a fabric assist zone
fazoneShow              Print Fabric Assist Zone information

cfgClear                Clear all zone configurations
cfgDisable              Disable a zone configuration
cfgEnable               Enable a zone configuration
cfgSave                 Save zone configurations in flash

cfgSize                 Print size details of zone database
cfgTransAbort           Abort zone configuration transaction
cfgTransShow            Print zone configurations in transaction buffer

switch:admin>
```

zoneremove

Remove a member from a zone.

Syntax `zoneremove "zonename", "member;member"`

Availability Admin

This command requires a Zoning license.

Description Use this command to remove one or more members from an existing zone.

The member list is located by an exact string match, therefore, it is important to maintain the order when removing multiple members. For example, if a zone contains `"array2; array3; array4"`, removing `"array3; array4"` succeeds. but removing `"array4; array3"` fails.

If all members are removed, the zone is deleted.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands The following operands are required:

zonename	Name of the zone, in quotation marks.
member	List of members to be removed from zone, in quotation marks, separated by semi-colons. Can be one or more of the following: • A switch domain and port area number pair. For example, `"2, 20"` View the area numbers for ports using the `switchshow` command. • Worldwide Names • QuickLoop AL_PAs • Zone alias names

Example To remove "array2" from "Blue_zone":

```
switch:admin> zoneremove "Blue_zone", "array2"
switch:admin> zoneremove "Blue_zone", "2,20"
```

See Also

```
zoneadd
zonecreate
zonedelete
zoneshow
```

zoneshow

Display zone information.

Syntax `zoneshow ["pattern"][, mode]`

Availability All users

This command requires a Zoning license.

Description Use this command to display zone configuration information.

If no parameters are specified, all zone configuration information (both defined and enabled) is displayed. Refer to `cfgshow` for a description of this display.

If a parameter is specified, it is used as a pattern to match zone configuration names, and those that match in the defined configuration are displayed.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands The following operand is optional:

pattern A POSIX style regular expression used to match zone configuration names. The pattern must be enclosed in quotation marks. Patterns may contain:

- Question mark "?" that matches any single character.
- Asterisk "*" that matches any string of characters.
- Ranges which match any character within the range. For example, [0-9] or [a-f].

mode Specify 0 to display the contents of the transaction buffer (the contents of the current transaction), or specify 1 to display the contents of the non-volatile memory. The default value is 0. This operand is optional.

Example **To show all zones beginning with the letters "A" through "C":**

```
switch:admin> zoneshow "[A-C]*"
zone: Blue_zone 1,1; array1; 1,2; array2
```

See Also

```
zoneadd
zonecreate
zonedelete
zoneremove
```

2

License Telnet Commands

This chapter summarizes the commands that are only available with a license key.

For more information about Zoning, Extended Fabrics, Fabric Watch, Trunking, or Performance Monitoring refer to the specific user guide for that feature.

Zoning Commands

The commands shown in Table 2-1 are available with the purchase of a Zoning license key. For detailed information about zoning, refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Zoning User Guide*.

Table 2-1 Zoning Commands

Command	Description
Zone Alias	
`aliadd`	Add a member to a zone alias.
`alicreate`	Create a zone alias.
`alidelete`	Delete a zone alias.
`aliremove`	Remove a member from a zone alias.
Zoning	
`zoneadd`	Add a member to a zone.
`zonecreate`	Create a zone.
`zonedelete`	Delete a zone.
`zoneremove`	Remove a member from a zone.
QuickLoop Zoning	
`qloopadd`	Add a member to a QuickLoop.
`qloopcreate`	Create a QuickLoop.
`qloopdelete`	Delete a QuickLoop.
`qloopremove`	Remove a member from a QuickLoop.
Zone Configuration	
`cfgadd`	Add a zone to a zone configuration.
`cfgcreate`	Create a zone configuration
`cfgdelete`	Delete a zone configuration

Table 2-1 Zoning Commands (*continued*)

Command	Description
`cfgremove`	Remove a zone from a zone configuration.
Zone Management	
`cfgclear`	Clear all zone configurations.
`cfgdisable`	Disable a zone configuration.
`cfgenable`	Enable a zone configuration.
`cfgsave`	Save zone configurations in flash memory.
`cfgtransabort`	Abort the current zoning transaction.

QuickLoop Fabric Assist Mode Commands

The commands shown in Table 2-2 are for QuickLoop Fabric Assist Mode. For detailed information about QuickLoop Fabric Assist refer to the *EMC Connectrix Departmental Switch DS-16B2 QuickLoop User Guide.*

Table 2-2 QuickLoop Fabric Assist Mode Commnands

Command	Description
`fazoneadd`	Add member(s) to an existing QuickLoop Fabric Assist zone.
`fazonecreate`	Creates a QLFA zone.
`fazonedelete`	Delete an existing QuickLoop Fabric Assist zone.
`fazoneremove`	Remove member or members from an existing QuickLoop Fabric Assist zone.

The QuickLoop Fabric Assist Mode feature is not available on Fabric OS v4.x.

Extended Fabric Command

The command shown in Table 2-3 is available with the purchase of a Extended Fabrics license key. For detailed information about Extended Fabrics refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Extended Fabrics User Guide*.

Table 2-3 Extended Fabric Command

Command	Description
`portcfglongdistance`	Configure a port to support long distance links.

Fabric Watch Commands

The commands shown in Table 2-4 are available with the purchase of a Fabric Watch license key. For detailed information about Fabric Watch, refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Fabric Watch User Guide*.

Table 2-4 Fabric Watch Commands

Command	Description
`fwclassinit`	Initialize all classes under Fabric Watch.
`fwconfigreload`	Reload the Fabric Watch configuration.
`fwconfigure`	Display and allows modification of the Fabric Watch configuration and status.
`fwshow`	Display the thresholds monitored by Fabric Watch.
`fwalarmsfilterset`	Enable or disable alarms for Fabric Watch.
`fwalarmsfiltershow`	Display alarm filtering for Fabric Watch.
`fwfrucfg`	Display and changes FRU state alert configuration.

Table 2-4 Fabric Watch Commands *(continued)*

Command	Description
`fwmailcfg`	Configure email alerts in Fabric Watch.
`fwsettocustom`	Set boundary and alarm levels to custom values.
`fwsettodefault`	Set boundary and alarm levels to default values.

Trunking Commands

The commands shown in Table 2-5 are available with the purchase of a Trunking license key. For more detailed information about trunking, refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B ISL Trunking User Guide*.

Table 2-5 Trunking Commands

Command	Description
`portcfgtrunkport`	Configure a port for trunking.
`switchcfgtrunk`	Configure a switch for trunking.
`trunkdebug`	Debug a trunking connection.

Performance Monitoring Commands

The commands shown in Table 2-6 are available with the purchase of an Advanced Performance Monitoring license key. For more detailed information about Performance Monitoring, refer to the *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director ED-12000B Performance Monitoring User Guide*.

Table 2-6 Performance Monitoring Commands

Command	Description
`perfaddeemonitor`	Add an end-to-end monitor to a port.
`perfaddipmonitor`	Add an IP monitor to a port.
`perfaddreadmonitor`	Add a SCSI Read monitor to a port.
`perfaddrwmonitor`	Add a SCSI Read and Write monitor to a port.
`perfaddscsimonitor`	Add a SCSI traffic frame monitor to a port.
`perfaddusermonitor`	Add a user-defined monitor to a port.
`perfaddwritemonitor`	Add a SCSI Write monitor to a port.
`perfcfgclear`	Clear the performance monitoring settings from flash memory.
`perfcfgrestore`	Restore performance monitoring settings from flash memory.
`perfcfgsave`	Save the current performance monitoring settings to flash memory.
`perfcleareemonitor`	Clear statistics counters of an end- to-end monitor on a port.
`perfclearfiltermonitor`	Clear statistics counters of a filter-based monitor.
`perfclralpacrc`	Clear an ALPA device CRC count by the port and ALPA.
`perfdeleemonitor`	Delete an end-to-end monitor on port.

Table 2-6 Performance Monitoring Commands (*continued*)

Command	Description
`perfdelfiltermonitor`	Delete a filter-based monitor.
`perfsetporteemask`	Set overall mask for end-to-end (EE) monitors.
`perfshowalpacrc`	Display the ALPA CRC count by port or by ALPA.
`perfshoweemonitor`	Display user-defined end-to-end monitors on a port.
`perfshowfiltermonitor`	Display filter-based monitors for a port.
`perfshowporteemask`	Display the current end-to-end mask of a port.

3 Fabric OS Version Comparison

This chapter summarizes the commands that are unique to Fabric OS v3.1 and v4.1.

Command Differences Between Versions

Table 3-1 provides a list of the commands that are unique to Fabric OS v4.1 and v3.1. It also provides notes on differences that may exist for a particular command between versions.

Table 3-1 Command Comparison between Fabric OS v4.1 and v3.1

Commands Found Only in v4.1	Commands Found Only in v3.1
	aliasdelete
	aliasjoin
	aliaspurge
	aliasshow
backplanetest	
backport	
	backspace
bladebeacon	
bladediag	
bladediagshort	
bladedisable	
bladeenable	
bladepropshow	
	bsn
chassisname	
chassisshow	
chippropshow	
chipregshow	
diagcommandshow	
diagesdports	
diagfaillimit	

Table 3-1 Command Comparison between Fabric OS v4.1 and v3.1 (*continued*)

Commands Found Only in v4.1	Commands Found Only in v3.1
diagloopid	
diagmodepr	
diagpost	
diagretry	
diagshowtime	
diagsilkworm	
diagskiptests	
errsavelvlset	
errsavelvlshow	
errnvlogsizeset	
errnvlogsizeshow	
fabportshow	
fabstateclear	
fabstateshow	
fabswitchshow	
fandisable	
fanenable	
	fashow
fastatsshow	
firmwarecommit	
firmwarerestore	
frureplace	
fwfrucfg	
	gbicshow
hadisable	

Table 3-1 Command Comparison between Fabric OS v4.1 and v3.1 (*continued*)

Commands Found Only in v4.1	Commands Found Only in v3.1
hadump	
haenable	
hafailover	
hashow	
hasyncstart	
hasyncstop	
historylastshow	
historymode	
historyshow	
	ifshow
itemlist	
killtelnet	
licenseidshow	
	mcastshow
myid	
	paritycheck
pdshow	
pkicreate	
pkiremove	
pkishow	
	portcamshow
portlogdisable	
portlogeventshow	
portlogreset	
portlogresize	

Table 3-1 Command Comparison between Fabric OS v4.1 and v3.1 (*continued*)

Commands Found Only in v4.1	Commands Found Only in v3.1
portlogtypedisable	
portlogtypeenable	
portstats64show	
portswap	
portswapdisable	
portswapenable	
portswapshow	
powerofflistset	
powerofflistshow	
ptdatashow	
ptphantomshow	
ptpropshow	
ptregshow	
ptrouteshow	
ptstatsshow	
	qldisable
	qlenable
	qlpartner
	qlportdisable
	qlportenable
	qlportshowall
	qlshow
	qlstatsshow
	quietmode
	ramtest

Table 3-1 Command Comparison between Fabric OS v4.1 and v3.1 (*continued*)

Commands Found Only in v4.1	Commands Found Only in v3.1
savecore	
seterrlvl	
setesdmode	
slotoff	
sloton	
slotpoweroff	
slotpoweron	
slotshow	
	ssn
switchdiag	
switchdiagshort	
switchreboot	
switchshutdown	
switchstart	
switchuptime	
systemverification	

4 Fabric and Switch Management

This chapter explains the different methods used to manage a storage area network (SAN) for DS-32B2 and ED-12000B switches.

Overview

The DS-32B2 and ED-12000B switches can be managed using several local and remote access methods. In order to manage a switch, you must have access to one of the available management methods:

- Fabric OS command line interface
- Web Tools
- Fabric Watch
- Management Server

Telnet, SNMP, and Web Tools require that the switch be accessible using a network connection. The network connection can be from the switch Ethernet port (out of band). The switch must be configured with an IP address to allow for the network connection. Refer to the hardware manual for your specific switch for information on physically connecting to the switch.

Before changing any of the factory default settings, become familiar with the operations described in this chapter, including both the switch functions and interactive characteristics.

Switches can be accessed simultaneously from different connections. If this happens, changes from one connection may not be updated to the other, and some modifications may be lost. Make sure when connecting with simultaneous multiple connections, that you do not overwrite the work of another connection.

User Access Level

There are two levels of user access for the DS-32B2 and ED-12000B switches.

- Admin
- User

In Fabric OS v4.0, each user access level can have the following number of simultaneous logins:

Table 4-1 DS-32B2 and ED-12000B User Access Maximum Sessions

User Name	Maximum Number of Simultaneous Sessions
Admin	2
User	4
Web Tools	4

In Fabric OS v3.0 and earlier, multiple user access to a switch is limited. Each switch allows only a single session per management access method, regardless of user level. Switches can, however, be accessed simultaneously from different connections (for example, through the CLI and Web Tools). If this happens, changes from one connection may not be updated to the other, and some changes may be lost. Make sure when connecting with simultaneous multiple connections, that you do not overwrite the work of another connection.

Fabric OS Command Line Interface

The Fabric OS command line interface (CLI) accessed through telnet or serial console provides the user with the full range of management capability on DS-32B2 and ED-12000B switches. The Fabric OS CLI enables an administrator to monitor and manage entire fabrics, individual switches, and ports from a standard workstation. The entire suite of Fabric OS features and capabilities is available across an entire fabric, from a single access point.

Access is controlled by a switch-level password for each user level (admin, user). The commands available through the CLI are based on the user's login level, and the license keys used to unlock certain features.

Generally speaking, all configuration and management tasks are available using the admin or user level ID. This manual lists all the commands available to the User and Admin level login IDs.

Fabric OS CLI is the complete fabric management tool for storage area networks (SANs), and provides the following advantages to administrators:

- Access to the full range of Fabric OS features, based on which license keys you purchase.
- A full set of tools to assist administrators with the configuration, monitoring, dynamic provisioning, and daily management of every aspect of SANs.
- Provides a deeper view of the tasks involved with managing DS-32B2 and ED-12000B switches.
- Configure and manage the fabric on multiple efficient levels.
- Identify, isolate, and manage SAN events across every switch in the fabric.
- Manage switch licenses
- Perform Fabric Stamping

Web Tools

Web Tools provides a graphical interface that allows the administrator to monitor and manage entire fabrics and individual switches and ports from a standard workstation. It is an optionally licensed product that runs on Fabric OS. All switches in the fabric are displayed in the main window of Web Tools, including switches that do not have a Web Tools license. However, only switches that have a Web Tools license installed can be managed through Web Tools (other switches must be managed through Telnet).

Web Tools is an excellent partner to the traditional Fabric OS CLI commands, and in many ways can provide faster and more effective results than can be achieved strictly through the CLI. Following are some of the features that make Web Tools an important part of the switch management and administration process:

- Web Tools can be used simultaneously with Fabric OS CLI commands. Simply open a second window and you can take advantage of the benefits of both interfaces at the same time.
- Web Tools can help you find the appropriate Fabric OS CLI command to perform a desired function. For instance, you can perform a function using Web Tools, and watch in a second window as the Fabric OS CLI commands are displayed.
- Web Tools can be used from a standard workstation and provides the user the advantage of being *virtually* in front of any fabric, switch, or port.
- Web Tools makes zoning a simple click and drag process, rather than having to tediously type out IP addresses and port numbers to put in a configuration.
- Web Tools provides the Performance Monitor feature. This feature allows you to view the status and traffic of a switch or port in seconds by easily creating a variety of effective graphs.
- Web Tools is easy and intuitive to use.

Fabric Watch

Fabric Watch software monitors the performance and status of Fibre Channel networks and DS-32B2 and ED-12000B switches, and can alert SAN managers when problems arise. The real-time alerts from Fabric Watch software help SAN managers solve problems before they become costly failures. SAN managers can configure Fabric Watch software to monitor any of the following:

- Fabric events (such as topology reconfigurations and zone changes)
- Physical switch conditions (such as fans, power supplies, and temperature)
- Port behavior (such as state changes, errors, and performance)
- SFPs behavior

With Fabric Watch software, SAN managers can place limits, or *thresholds*, on the behavior of different switch and fabric elements. Fabric Watch then monitors these behavior variables, or *counters*, and issues an alarm to address problems when a counter exceeds a threshold. An alarm may email the SAN manager or lock out a port log, depending on how the manager configures the alarm.

Management Server

The Management Server allows an Storage Area Network (SAN) management application to retrieve and administer the fabric and interconnect elements such as switches, servers, and storage devices.

An access control list (ACL) of WWN addresses determines which systems have access to the Management Server database. If the list is empty (default), the Management Server is accessible to all systems connected in-band to the fabric. For a more secured access, an administrator may specify WWNs in the ACL. These WWNs are usually associated with the management applications. If any WWNs are entered into the ACL, then access to the Management Server is restricted to only those WWNs listed in the ACL.

5

Control Processor Commands

This chapter lists the commands available when logged into the Active CP and Standby CP in an ED-12000B.

Active CP Commands

When logged into the Active CP, the full suite of commands are supported (subject to which license keys are installed).

When logged in to the Active CP, most commands are still specific to a single logical switch. That is, they are executed on one logical switch but not the other. If you are logged in to the Active CP through the console port, you are prompted to specify the logical switch on which commands are executed on. If you log in to the Active CP through the Fabric OS Telnet shell, commands always execute on the default switch (logical switch 0).

Some commands, when executed from the Active CP, affect the entire chassis. For example, when the `reboot` command is issued on the Active CP, the command reboots both logical switches and the Active CP.

Standby CP Commands

The following commands are supported when logged in to the Standby CP.

Table 5-1 ED-12000B Standby CP Commands

Command	Notes
`date`	Print/set the system date and time.
`errclear`	Clear error log.
`errdump`	Print error log (no page breaks).
`errnvlogsizeset`	Resize non-volatile (persistent) error log.
`errnvlogsizeshow`	Show persistent error log configuration.
`errsavelvlset`	Set error save level.
`errsavelvlshow`	Get error save level.
`errshow`	Print error log.
`fastboot`	Reboot this switch, bypassing POST.
`firmwarecommit`	Commit firmware to stable storage.
`firmwaredownload`	Download firmware into switch.
`firmwaredownloadstatus`	Display the progress and status of firmwaredownload.
`firmwarerestore`	Restore the old firmware in the switch.
`firmwareshow`	Display firmware versions in the switch.
`h`	Print shell history.
`hadump`	Dump HA debug data.
`hashow`	Print High availability status.
`help`	Print this list.
`ifmodeset`	Set the link operating mode for a network interface.
`ifmodeshow`	Display the link operating mode for a network interface.

Table 5-1 ED-12000B Standby CP Commands (*continued*)

`killtelnet`	Terminate telnet/serial login sessions interactively.
`memshow`	Display memory usage in the system.
`myid`	Display the current login session details.
`pdshow`	Show information from Panic Dump file.
`reboot`	Reboot the Standby CP.
`savecore`	FTP or Remove core files generated by daemons.
`switchname`	Print this switch's name.
`tstimezone`	Display Time Zone.
`uptime`	Print how long switch has been up.
`version`	Print firmware version.

6

Security and Commands

This chapter summarizes the commands that are only available on the primary FCS when the security feature is enabled.

Commands Exclusive to the Primary FCS

The commands shown in Table 6-1 are available only on the Primary FCS when security is installed and enabled.

Table 6-1 Commands Exclusive to the Primary FCS

Command	Notes
agtcfgset	Can be run on all switches, but it needs to be run on the Primary FCS to modify community strings
agtcfgdefault	Must be run from the Primary FCS switch.
aliadd	Must be run from the Primary FCS switch.
alicreate	Must be run from the Primary FCS switch.
alidelete	Must be run from the Primary FCS switch.
aliremove	Must be run from the Primary FCS switch.
alishow	Must be run from the Primary FCS switch.
cfgadd	Must be run from the Primary FCS switch.
cfgclear	Must be run from the Primary FCS switch.
cfgcreate	Must be run from the Primary FCS switch.
cfgdelete	Must be run from the Primary FCS switch.
cfgdisable	Must be run from the Primary FCS switch.
cfgenable	Must be run from the Primary FCS switch.
cfgremove	Must be run from the Primary FCS switch.
cfgsave	Must be run from the Primary FCS switch.
cfgshow	Can be run on all FCS switches.
cfgtransabort	Must be run from the Primary FCS switch.
cfgtransshow	Must be run from the Primary FCS switch.
date	This command can be run on all switches to view the current date. You can only modify the date from the Primary FCS switch.

Table 6-1 Commands Exclusive to the Primary FCS (continued)

Command	Notes
fazoneadd	Must be run from the Primary FCS switch.
fazonecreate	Must be run from the Primary FCS switch.
fazonedelete	Must be run from the Primary FCS switch.
fazoneremove	Must be run from the Primary FCS switch.
fazoneshow	Must be run from the Primary FCS switch.
msconfigure	Can be run on all switches, but it does not dislay ACL in Secure Mode.
msplmgmtdeactivate	Must be run from the Primary FCS switch.
msplmgmtactivate	Must be run from the Primary FCS switch.
msplcleardb	Must be run from the Primary FCS switch.
mstddisable	mstddisable "ALL" must be run from the Primary FCS switch.
mstdenable	mstdenable "ALL" must be run from the Primary FCS switch.
passwd	Must be run from the Primary FCS switch.
qloopadd	Must be run from the Primary FCS switch.
qloopcreate	Must be run from the Primary FCS switch.
qloopdelete	Must be run from the Primary FCS switch.
qloopremove	Must be run from the Primary FCS switch.
qloopshow	Must be run from the Primary FCS switch.
secfabricshow	Must be run from the Primary FCS switch.
secmodedisable	Must be run from the Primary FCS switch.
secnonfcspasswd	Must be run from the Primary FCS switch.
secpolicyabort	Must be run from the Primary FCS switch.
secpolicyactivate	Must be run from the Primary FCS switch.
secpolicyadd	Must be run from the Primary FCS switch.
secpolicycreate	Must be run from the Primary FCS switch.

Table 6-1 Commands Exclusive to the Primary FCS (continued)

Command	Notes
secpolicydelete	Must be run from the Primary FCS switch.
secpolicydump	Can be run on all FCS switches.
secpolicyfcsmove	Must be run from the Primary FCS switch.
secpolicyremove	Must be run from the Primary FCS switch.
secpolicysave	Must be run from the Primary FCS switch.
secpolicyshow	Can be run on all FCS switches.
sectemppasswdset	Must be run from the Primary FCS switch.
sectemppasswdreset	Must be run from the Primary FCS switch.
secversionreset	Must be run from the Primary FCS switch. Can also be run on a single non-FCS switch which is segmented from a fabric.
tsclockserver	Can be run on all switches to view the NTP server's IP address. You can only modify the NTP server's IP address on the Primary FCS switch.
wwn	This command can be run on all switches to view the WWN. With security enabled the WWN of a switch cannot be modified.
zoneadd	Must be run from the Primary FCS switch.
zonecreate	Must be run from the Primary FCS switch.
zonedelete	Must be run from the Primary FCS switch.
zoneremove	Must be run from the Primary FCS switch.
zoneshow	Must be run from the Primary FCS switch.

7 Supportshow Reference

This chapter explains the information displayed by the `supportshow` command.

Supportshow Control Commands

The `supportshow` command is used to display support information by executing groups of pre-selected Fabric OS and LINUX commands. The information displayed by the `supportshow` command can be controlled by a set of control commands:

`supportshowcfgshow`
: Display which groups of commands are enabled to display under `supportshow`.

`supportshowcfgenable`
: Enable a group of commands to display under `supportshow`.

`supportshowcfgdisable`
: Disable a group of commands from displaying under `supportshow`.

Supportshow Command Groups

Table 7-1 displays the command groups under `supportshow`, and which Fabric OS or Linux commands are executed by that group.

Many of the commands executed by `supportshow` are intended for support use only. These commands are not intended for end users.

Table 7-1 Supportshow Command Groups

Command Group	Fabric OS v3.1	Fabric OS v4.1
os	mqshow i memshow mallocshow fastcheckheap	mii-tool -vv /usr/bin/du -xh / | /bin/sort: /bin/ps -elfh /bin/echo /bin/rpm -qa /bin/cat /var/log/dmesg /bin/cat /etc/fstab /bin/cat /etc/mtab printing proc entries. Refer to for more information.
exception	faultshow traceshow errdump	errdump -a/-p
port	portshow portregshow portstructshow bloomdatashow portrouteshow portsemshow bloomsemshow semashow 1	diagshow portshow portloginshow protregshow portrouteshow

Table 7-1 Supportshow Command Groups (continued)

Command Group	Fabric OS v3.1	Fabric OS v4.1
fabric	fabricshow islshow trunkshow topologyshow fashow qlshow cfgshow fabstatsshow fablogdump	fabricshow islshow trunkshow toplogyshow fabstateshow fabswitchshow fabstatsshow fabportshow fspfshow fcplogshow /fabos/bin/zone stateshow portzoneshow portcamshow cfgsize cfgshow rcssmshow rcsinfoshow rcsregistryshow
services	nsshow nsallshow nscamshow	nsshow nsallshow fdmishow fdmicacheshow
security	secmodeshow secpolicydump secstatsshow secfabricshow	secmodeshow secpolicydump secstatsshow secfabricshow
network	ipaddrshow ifshow ipstatshow udpstatshow tcpstatshow inetstatshow mbufshow arpshow routeshow routestatshow hostshow feidumpprint i557dump feiiteraterfdrings	/sbin/bootenv /sbin/sin /bin/df /sbin/ifconfig /sbin/route /bin/hostname

Table 7-1 Supportshow Command Groups (continued)

Command Group	Fabric OS v3.1	Fabric OS v4.1
portlog	portlogdump (no parameters) portlogdump 0, 1	portlogdump
system	version uptime switchshow tempshow psshow licenseshow diagshow portflagsshow porterrshow portcfgshow configshow	myid version firmwareshow uptime switchstatusshow switchshow hadump tempshow sensorshow psshow fanshow licenseshow portflagshow portcfgshow sfpshow porterrshow fwsamshow agtcfgshow chassisshow switchstatuspolicyshow fwalarmsfiltershow timeout historyshow configshow
extend	bloomlistdisplay bloomfdetshow bloomramdump	ptbufshow ptcreditshow ptdatashow ptphantomshow ptpropshow ptstatsshow
filter	filtershow	filterportshow
perfmon	ps_dump	ps_dump -a -n port#

Proc Entry Information Displayed

The os command group prints a number of proc entries. Table 7-2 presents example proc entry information displayed.

Table 7-2 Proc Entry Information Displayed

Proc Display Command	Proc Example Display
/proc/cmdline	/proc/cmdline quiet
/proc/cpuinfo	/proc/cpuinfo cpu : 405GP clock : 200MHz revision : 1.69 (pvr 4011 0145) bogomips : 199.47 machine : Brocade Silkworm plb bus clock : 100MHz pci bus clock : 33MHz

Table 7-2 Proc Entry Information Displayed

Proc Display Command	Proc Example Display
/proc/devices	/proc/devices Character devices: 1 mem 2 pty 3 ttyp 4 ttyS 5 cua 7 vcs 10 misc 89 i2c 90 mtd 128 ptm 136 pts 162 raw 245 swd 246 ham 247 fc 248 fc-switch 249 fabsys 250 fss_kt 251 fss_data 252 fss_mgmt 253 portlog 254 platform Block devices: 1 ramdisk 3 ide0 7 loop
/proc/filesystems	/proc/filesystems nodev rootfs nodev bdev nodev proc nodev sockfs nodev tmpfs nodev shm nodev pipefs ext2 nodev ramfs nodev nfs nodev devpts xfs nodev dfs

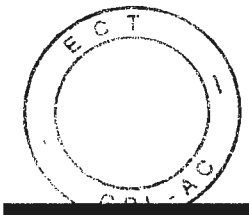


Table 7-2 Proc Entry Information Displayed

Proc Display Command	Proc Example Display
/proc/interrupts	/proc/interrupts CPU0 0: 0 IBM UIC Level serial 1: 591 IBM UIC Level serial 2: 2696197 IBM UIC Level IBM OCP IIC 10: 0 IBM UIC Level OCP EMAC MAL SERR 11: 1512 IBM UIC Level OCP EMAC TX EOB 12: 343895 IBM UIC Level OCP EMAC RX EOB 13: 0 IBM UIC Level OCP EMAC TX DE 14: 0 IBM UIC Level OCP EMAC RX DE 26: 52017 IBM UIC Level bloom 30: 1060300 IBM UIC Level ide0 FIT: 0 PIT: 15879069 BAD: 0
/proc/meminfo	/proc/meminfo total: used: free: shared: buffers: cached: Mem: 129740800 97079296 32661504 0 118784 45764608 Swap: 0 0 0 MemTotal: 126700 kB MemFree: 31896 kB MemShared: 0 kB Buffers: 116 kB Cached: 44692 kB SwapCached: 0 kB Active: 23464 kB Inactive: 49472 kB HighTotal: 0 kB HighFree: 0 kB LowTotal: 126700 kB LowFree: 31896 kB SwapTotal: 0 kB SwapFree: 0 kB
/proc/modules	/proc/modules dubby-module 582614 2 chubby-module 3128618 126 [dubby-module] dfs 5458 1 [dubby-module] consolelog-module 8539 0 (unused) panicdump-module 15279 0 [chubby-module consolelog-module] xfsnotificationhandler 4858 0 (unused)

Table 7-2 Proc Entry Information Displayed

Proc Display Command	Proc Example Display
/proc/mounts	/proc/mounts rootfs / rootfs rw 0 0 dev/hda1 / xfs rw,noatime 0 0 /proc /proc proc rw 0 0 none /dev/pts devpts rw 0 0 none /tmp ramfs rw 0 0 /dev/hda2 /mnt xfs rw,noatime 0 0 /diag /diag dfs rw 0 0
/proc/mtd	/proc/mtd dev: size erasesize name mtd0: 00010000 00010000 "boot environment" mtd1: 00070000 00010000 "boot prom" mtd2: 01000000 00040000 "Entire user flash" mtd3: 00400000 00040000 "kernel and initrd (1)" mtd4: 00400000 00040000 "kernel and initrd (2)" mtd5: 00400000 00040000 "log data (1)" mtd6: 00400000 00040000 "log data (2)"
/proc/partitions	/proc/partitions major minor #blocks name 3 0 250880 hda 3 1 124912 hda1 3 2 124928 hda2

Table 7-2 Proc Entry Information Displayed

Proc Display Command	Proc Example Display
/proc/pci	/proc/pci PCI devices found: Bus 0, device 0, function 0: Host bridge: IBM 405GP PLB to PCI Bridge (rev 1). Master Capable. Latency=7. Prefetchable 32 bit memory at 0x0 [0x7fffffff]. Bus 0, device 4, function 0: IDE interface: CMD Technology Inc PCI0649 (rev 2). IRQ 30. Master Capable. Latency=64. Min Gnt=2.Max Lat=4. I/O at 0x1008 [0x100f]. I/O at 0x1000 [0x1003]. I/O at 0x2000 [0x2007]. I/O at 0x3000 [0x3003]. I/O at 0x4000 [0x400f]. Bus 0, device 6, function 0: Non-VGA unclassified device: Brocade Communications Systems, Inc. Bloom switch (rev 0). IRQ 26. --<output truncated>--
/proc/slabinfo	/proc/slabinfo slabinfo - version: 1.1 kmem_cache 74 102 112 3 3 1 ip_mrt_cache 0 0 96 0 0 1 tcp_tw_bucket 2 40 96 1 1 1 tcp_bind_bucket 5 113 32 1 1 1 tcp_open_request 0 59 64 0 1 1 inet_peer_cache 1 59 64 1 1 1 ip_fib_hash 11 113 32 1 1 1 ip_dst_cache 65 168 160 7 7 1 arp_cache 2 30 128 1 1 1 blkdev_requests 128 160 96 4 4 1 xfs_chashlist 193 404 16 2 2 1 xfs_ili 2004 5668 152 135 218 1 xfs_ifork 0 0 56 0 0 1 xfs_efi_item 0 12 328 0 1 1 xfs_efd_item 0 12 328 0 1 1 --<output truncated>--

Table 7-2 Proc Entry Information Displayed

Proc Display Command	Proc Example Display
/proc/stat	/proc/stat cpu 184683 47107 88647 15558673 cpu0 184683 47107 88647 15558673 page 54635 71305 swap 0 0 intr 4154525 0 591 2696197 0 0 0 0 0 0 0 0 1520 343900 0 0 0 0 0 0 0 0 0 0 0 0 0 52017 0 0 0 1060300 0 disk_io: (3,0):(61121,5352,115463,55769,944835) ctxt 44089966 btime 1048729603 processes 17684
/proc/tty/drivers	/proc/tty/drivers serial /dev/cua 5 64-65 serial:callout serial /dev/ttyS 4 64-65 serial pty_slave /dev/pts 136 0-255 pty:slave pty_master /dev/ptm 128 0-255 pty:master pty_slave /dev/ttyp 3 0-255 pty:slave pty_master /dev/pty 2 0-255 pty:master /dev/vc/0 /dev/vc/0 4 0 system:vtmaster /dev/ptmx /dev/ptmx 5 2 system /dev/console /dev/console 5 1 system:console /dev/tty /dev/tty 5 0 system:/dev/tty
/proc/uptime	/proc/uptime 158791.21 155710.77
/proc/version	/proc/version Linux version 2.4.19 (swrel@sierra) (gcc version 2.95.3 20010112 (prerelease)) #1 Wed Mar 26 00:04:35 PST 2003

A

Customer Support

This appendix reviews the EMC process for detecting and resolving software problems, and provides essential questions that you should answer before contacting the EMC Customer Support Center.

This appendix covers the following topics:

Overview of Detecting and Resolving Problems

EMC software products are supported directly by the EMC Customer Support Center in the United States.

EMC uses the following process to resolve customer problems with its software products (Figure A-1).

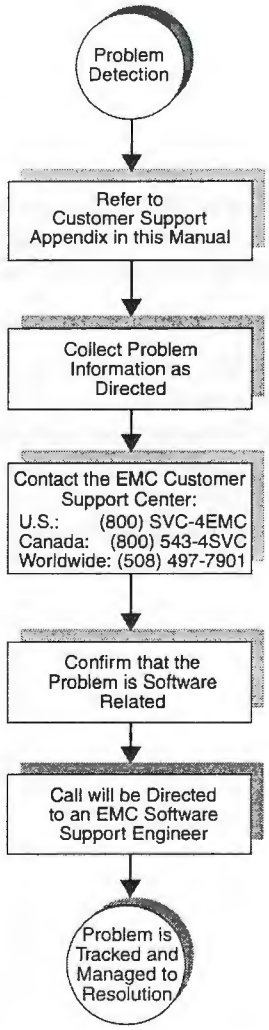


Figure A-1 Problem Detection and Resolution Process

Troubleshooting the Problem

Please perform the relevant diagnostic steps before you contact the EMC Customer Support Center:

1. Read the documentation carefully.
2. Reconstruct the events leading up to the problem and describe them in writing.
3. Run some test cases to reproduce the problem.

If you encounter a problem that requires technical programming or analysis, call the nearest EMC office or contact the EMC Customer Support Center at one of the following numbers:

United States: **(800) 782-4362 (SVC-4EMC)**

Canada: **(800) 543-4782 (543-4SVC)**

Worldwide: **(508) 497-7901**

Please do not request a specific support representative unless one has already been assigned to your particular system problem.

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink Web site at:

```
http://powerlink.emc.com
```

Before Calling the Customer Support Center

Have the following information available before calling the Customer Support Center or your support representative (if one has been assigned to you):

- ❑ Your company name
- ❑ Your name
- ❑ Your phone number
- ❑ For an existing problem, the problem tracking system ID, if one was previously assigned to the problem by a support representative

Documenting the Problem

If the EMC Customer Support Center requests information regarding the problem, please document it completely, making sure to include the following information:

- ❑ Your company name and address
- ❑ Your name
- ❑ Your telephone number
- ❑ The importance of the problem, so that it can be assigned a priority level

To expedite the processing of your support request, you can photocopy this list and include it with the package.

Reporting a New Problem

For a new problem, please provide the following information:

- ❑ Release level of the software that you are running
- ❑ Software installation parameters
- ❑ Host type on which you are running
- ❑ Operating system you are running and its release number
- ❑ Functions of the software that you are running
- ❑ Whether you can reproduce the problem
- ❑ Previous occurrences of the problem
- ❑ Whether the software has ever worked correctly
- ❑ Time period that the software did work properly
- ❑ Conditions under which the software worked properly
- ❑ Changes to your system between the time the software worked properly and the problem began
- ❑ Exact sequence of events that led to the system error
- ❑ Message numbers and complete text of any messages that the system produced
- ❑ Log file dated near the time the error occurred
- ❑ Results from tests that you have run
- ❑ Other related system output
- ❑ Other information that may help solve the problem

Sending Problem Documentation

Use one of the following methods to send documentation of the problem to the EMC Customer Support Center:

- Email
- FTP
- U.S. Mail to the following address:

  EMC Customer Support Center
  45 South Street
  Hopkinton, MA 01748-9103

  If the problem was assigned a number or a specific support representative, please include that information in the address as well.

BB_Credit 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* and *EE_Credit*.

Beacon When all the port 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 the 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 Bit error rate. 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 See *16-Port Card*.

Block As applies to Fibre Channel, upper-level application data that is transferred in a single sequence.

Blower Assembly A fan that prevents a switch (or individual elements within a switch) from over heating.

Boot Flash Flash memory that stores the boot code and boot parameters. The processor executes its first instructions from boot flash. Data is cached in RAM.

Boot Monitor Code used to initialize the CP (control processor) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

Broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *Multicast* and *Unicast*.

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 *BB_Credit*.

C

Cascade The interconnection means through which data flows from one switch to another in a fabric.

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 The class of frame-switching service that provides a dedicated connection between two communicating ports (also called connection- oriented service), with acknowledgment of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgment of delivery or nondelivery of frames.

Class 3 A connectionless frame switching service that does not include acknowledgment of delivery or nondelivery of frames. Can be used to provide a multicast connection between the originator and recipients, with acknowledgment of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

Class of Service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through Telnet or SNMP, and does not involve a graphical user 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*.

Glossary

The terms in the glossary relate to the switch and Fibre Channel connections. Many of these terms are used in this manual.

Numbers

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 ED-12000B. Contains 16 fibre channel ports and the corresponding LEDs indicating port status and speed. See also *Port Card*.

A

Access Control List Enables an organization to bind a specific 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. May also refer to a list of the read/write access of a particular community string. See also *Device Connection Controls*.

Address Identifier A 24-bit value 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.

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 WWNs when creating zones.

Alias Address Identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports.

Alias Server A fabric software facility that supports multicast group management.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

ANSI American National Standards Institute. The governing body for Fibre Channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

Arbitrated Loop A shared Fibre Channel transport structured as a loop. Supports up to 126 devices and one fabric attachment. See also *Topology.*

Area Number A number assigned to each potential port location in the ED- 12000B. Used to distinguish ED- 12000B ports that have the same port number but are on different port cards.

ASIC Application-specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

Auto-Negotiate Speed Process that allows two devices at either end of a link segment to negotiate common features, speed (e.g., 1 or 2 Gb/s) and functions.

Autosense Process during which a network device automatically senses the speed of another device.

B

Backup FCS Switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS Switch* and *Primary FCS Switch.*

Bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a network. See also *Throughput.*

Community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. See also *SNMP*.

Compact Flash Flash memory that stores the run time operating system and is used like hard disk storage. Not visible within the processor's memory space. Data is stored in file system format.

Configuration How a system is set up. May refer to hardware or software.

Hardware: The number, type, and arrangement of components that make up a system or network.

Software: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

Connection Initiator A port that has originated a Class 1 dedicated connection and received a response from the recipient.

Connection Recipient A port that has received a Class 1 dedicated connection request and transmitted a response to the originator.

Control Panel Refers to the left-side panel of Web Tools, which accesses fabric-wide functions such as zoning and events.

Core Switch A switch whose main task is to interconnect other switches. See also *Edge Switch*.

CP Card Control processor card. The central processing unit of the ED-12000B contains two CP card slots to provide redundancy. Provides ethernet, serial, and modem ports with the corresponding LEDs.

CRC Cyclic redundancy check. A check for transmission errors included in every data frame.

Credit As applies to Fibre Channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit* and *EE_Credit*.

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*

D

Data Word Type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *Frame*, *Ordered Set*, and *Transmission Word*.

DB-9 Connector A 9-pin version of the RS-232C port interface. May be either the male or female interface. See also *RS-232 Port*.

dBm, dBW Logarithmic units of power used in electronics. Indicates signal strength in decibels above the reference level, which is 1 milliwatt for dBm, and 1 watt for dBW. An increase of 10 dBm or 10 dBW represents a 10-fold increase in power.

DCE Port A data communications equipment port capable of interfacing between a DTE (data terminal equipment) port and a transmission circuit. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *DTE Port* and *RS-232 Port*.

Defined Zone Configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *Zone Configuration*.

Device A disk, a RAID, or an HBA.

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 WWN and typically represent HBAs (servers). See also *Access Control List*.

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 Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

Domain ID As applies to Departmental Switches, a unique number between 1 and 239 that identifies the switch to the fabric and is used in routing frames. Usually automatically assigned by the switch, but can be manually assigned.

DTE Port A data terminal equipment port capable of interfacing to a transmission circuit through a connection to a DCE (data communications equipment) 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 connection (reversed in 25-pin connectors). See also *DCE Port* and *RS-232 Port*.

DWDM Dense wavelength multiplexing. A means to concurrently transmit more than one stream of data through a single fiber by modulating each stream of data on to a different wavelength of light.

E

Edge Switch A switch whose main task is to connect nodes to the fabric. See also *Core Switch*.

E_D_TOV Error detect time-out value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error condition is declared. See also *R_A_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

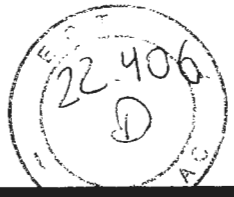
EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *End-to-End Flow Control* and *BB_Credit*.

Effective 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*.

EIA Rack A storage rack that meets the standards set by the Electronics Industry Association.

End-to-End Flow Control Governs flow of Class 1 and 2 frames between N_Ports. See also *EE_Credit*.

Error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).



ESN Enterprise Storage Network. A storage network implementation that integrates products, technology, and services offering universal data access for every major computing platform, operating system, and application across any combination of SCSI, Ultra SCSI, Fibre Channel, and ESCON technologies.

Exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in one or both directions.

Extended Fabrics A product that runs on Fabric OS and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 kilometers.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. See also *FL_Port* and *Fx_Port*.

Fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *Topology*, *ESN*, and *Cascade*.

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 Name The unique identifier assigned to a fabric and communicated during login and port discovery.

Failover The act that causes control to pass from one redundant unit to another.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCIA Fibre Channel Industry Association. An international organization of Fibre Channel industry professionals. Provides oversight of ANSI and industry-developed standards, among other tasks

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCP Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS Switch Fabric configuration server 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 WWN, and the list of designated switches is communicated fabric-wide. See also *Backup FCS Switch* and *Primary FCS 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 Transport A protocol service that supports communication between Fibre Channel service providers. See also *FSP*.

FIFO First in, First out. May also refer to a data buffer that follows the first in, first out rule.

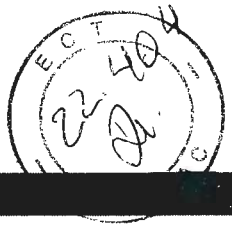
Fill Word An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

Firmware The basic operating system provided with the hardware.

Firmware Download The process of loading firmware down from a server into the switch.

Flash Programmable NVRAM memory that maintains its contents.

Flash Partition Two redundant usable areas, called partitions, into which firmware can be downloaded.



FLOGI Fabric Login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI*.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. See also *F_Port* and *Fx_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, etc.) and data frames.

FRU Field replaceable unit. A component that can be replaced on site.

FS Fibre Channel Service. 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 *FSP*.

FSP Fibre Channel Service Protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.

FSPF Fabric Shortest Path First. A routing protocol for Fibre Channel switches.

Full Duplex A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *Half Duplex*.

Full Fabric The EMC software license that allows multiple E_Ports on a switch, making it possible to create multiple ISLs.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port* and *FL_Port*.

G

G_Port Generic port. A port that can operate as either an E_Port or 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.

Gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical level transport for Fibre Channel and Gigabit Ethernet. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *SFP*.

Gb/s Gigabits per second (1,062,500,000 bits/second).

GB/s GigaBytes per second (1,062,500,000 bytes/second).

H

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*.

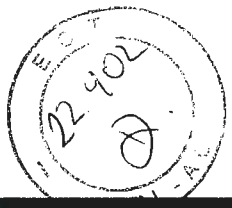
HBA Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

High Availability An attribute of equipment that identifies it as being capable of conducting customer operations well in excess of 99% of the time. Typically, high availability is identified by the number of nines in that percentage. Five nines means the equipment is rated as being capable of conducting customer operations 99.999% of the time without failure.

Host A computer that accesses storage devices over the fabric. May also be referred to as a server. See also *Workstation*.

Hot Pluggable A FRU capability that indicates it may 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.



I

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.

Initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *Target*.

Integrated Fabric The fabric created by connecting multiple switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. See also *E_Port* and *Cascade*.

Isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port*.

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

J

JBOD Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. See also *RAID*.

K

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 processor's memory space. Data is stored as raw bits.

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or nonparticipating mode.

See also *Nonparticipating Mode* and *Participating Mode*.

Latency The period of time required to transmit a frame, from the time it is sent until it arrives.

LED Light-emitting diode. Used to indicate status of elements on switch.

Link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *Circuit*.

Link Services A protocol for link-related actions.

LWL Long wavelength. A type of fiber-optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *SWL*.

M

Media See *Transceiver*.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Modem Serial Port The upper serial port on the CP card. Can be used to connect the CP card to a country-specific modem. Has a DB-9 connector wired as a ttyS1 DTE device, and can be connected by serial cable to a DCE device. Can be connected to a modem using a standard 9-pin modem cable. A Hayes-compatible modem or Hayes-emulation is required. See also *DCE Port* and *Terminal Serial Port*.

Multicast The transmission of data from a single source to multiple specified 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 meters for 1 GB Fibre Channel and 300 meters for 2 GB Fibre Channel between devices.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. See also *NL_Port* and *Nx_Port*.

Name Server The term frequently used to indicate Simple Name Server. See also *SNS*.

Node A Fibre Channel device that contains an N_Port or NL_Port.

Negotiate See *Auto-Negotiate Speed* and *Autosense*.

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. See also *N_Port* and *Nx_Port*.

Nonparticipating Mode A mode in which an 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 AL_PA cannot be acquired. See also *L_Port* and *Participating Mode*.

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

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 the following items:

- Frame delimiters mark frame boundaries and describe frame contents.
- Primitive signals indicate events.
- Primitive sequences indicate or initiate port states.

Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames.

P

Packet A set of information transmitted across a network. See also *Frame*.

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. See also *L_Port* and *Nonparticipating Mode*.

Path Selection The selection of a transmission path through the fabric. EMC switches use the FSPF protocol.

PLOGI Port Login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI*.

Point-to-Point A Fibre Channel topology that employs direct links between each pair of communicating entities. See also *Topology*.

Port_Name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

Port Cage The metal casing extending out of the optical port on the switch, and in which the GBIC or SFP can be inserted.

Port Card A Fibre Channel card that contains optical port interfaces. See also *16-Port Card*.

Port Module A collection of ports in a switch.

POST Power-on self test. A series of tests run by a switch after it is turned on.

Principal Switch The switch that assumes the responsibility to assign Domain IDs. The role of Principle Switch is negotiated after a Build Fabric event.

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*.

Private Device A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log in to the fabric.

Private Loop An arbitrated loop that does not include a participating FL_Port.

Private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to 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 in to the fabric.

Public Loop An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.

Public NL_Port An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.

Q

Quad A group of four adjacent ports that share a common pool of frame buffers.

R

R_A_TOV Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV*.

R_RDY Receiver ready. A primitive signal indicating that the port is ready to receive a frame.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. See also *JBOD*.

Remote Fabric A fabric that spans across WANs by using protocol translation (a process also known as tunneling) such as Fibre Channel over ATM or Fiber Channel over IP.

Request Rate The rate at which requests arrive at a servicing entity. See also *Service Rate*.

Root Account A login used for debugging purposes and is not intended for customer use.

Route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. See also *SFP*.

Routing The assignment of frames to specific switch ports, according to frame destination.

RS-232 Port A port that conforms to a set of EIA (Electrical Industries Association) standards. Used to connect DTE and DCE devices for communication between computers, terminals, and modems. See also *DCE Port* and *DTE Port*.

RSCN Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

S

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. See also *Fabric*.

SCSI Small computer systems interface. A parallel bus architecture and protocol for transmitting large data blocks to a distance of 15-25 meters.

SDRAM Synchronous dynamic random access memory. The main memory for the switch. Used for volatile storage during switch operation. See also *Flash*.

Sequence A group of related frames transmitted in the same direction between two N_Ports.

Service Rate The rate at which an entity can service requests. See also *Request Rate*.

SES A Brocade product that runs on Fabric OS and allows monitoring, configuring, and maintenance of the Departmental Switch family using SCSI 3 Enclosure Services.

SFP Small form factor pluggable. Optical transceiver used to convert signals between optical fiber cables and switches. GBIC and SFP terms are used interchangeably throughout the documentation, although they are different types of optics and the hardware is not interchangeable. See also *GBIC*.

SI Sequence initiative.

SID/DID Source identifier/destination identifier. S_ID is a 3-byte field in the frame header that is used to indicate the address identifier of the N_Port from which the frame was sent.

Single Mode A Fibre Channel optic cabling standard for use with long-wavelength lasers operating in the infrared portion of the spectrum at 1300 nonmeters (nm).

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. See also *Community (SNMP)*.

SNS Simple Name Server. 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. May also be referred to as directory service. See also *FS*.

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 E_Ports, F_Ports, or FL_Ports.

SWL Short wavelength. A type of fiber-optic cabling that is based on 850mm lasers and supports link speeds of 1.0625 Gb/s and 2.125 Gb/s. May also refer to the type of GBIC or SFP. See also *LWL*.

T

Target A storage device on a Fibre Channel network. See also *Initiator*.

Terminal Serial Port The lower serial port on the CP card. Receives error messages. Can be used to connect the CP card to a computer terminal. Has a DB-9 connector wires as a ttyS0 DTE device, and can be connected by serial cable to a DCE device. The connector has pins two and three swapped so that a straight-through cable can be used to connected to a terminal. See also *DB-9 Connector*, *DCE Port*, and *Modem Serial Port*.

Throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *Bandwidth*.

Topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point-to-point — A direct link between two communication ports.
- Switched fabric — Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop — Multiple NL_Ports connected in a loop.

Transceiver Device that converts one form of signaling to another for transmission and reception. In fiber optics, it refers to optical and electrical.

Transmission Character A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Word A group of four transmission characters.

Trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

Tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or 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.

UDP User Datagram Protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level Protocol. The protocol that runs on top of Fibre Channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

Unicast The transmission of data from a single source to a single destination. See also *Broadcast* and *Multicast*.

User Account A login intended for use by the customer to monitor, but not control, switch operation.

V

VC Virtual circuit. A one-way path between N_Ports that allows fractional bandwidth.

W

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.

Workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

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.

Zone Alias A name assigned to a device or group of devices in a zone. Aliases can greatly simplify the zone administrative process.

Zone Configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. See also *Defined Zone Configuration*.

Zone Member A port, node, WWN, or alias, which is part of a zone.

Zone Schemes The level of zoning granularity selected. For example, zoning may be done by switch/port, WWN, or a mixture. See also *Zone Configuration*.

Zone Set See *Zone Configuration*.

Index

COBRA TECNOLOGIA

Integradora de Soluções em TI e Serviços

ANEXO SWITCH TIPO 03
PARTE 4/A

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

Connectrix B Fabric Manager

Version 4.0

USER GUIDE

P/N 069001220
REV A01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748 -9103
1-508 -435 -1000
www.EMC.com

Printed July, 2003

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Regulatory Agency Information

EMC Connectrix B Fabric Manager has been extensively tested and certified to meet UL60950, CSA 22.2 No 60950, IEC 60950/EN60950; Safety of Information Technology Equipment including Electrical Business Equipment, FCC Rules Part 15 Subpart B; CISPR22 Class A; European EMC Directive 89/336/EEC on, electromagnetic compatibility.

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning!
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.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

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。

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

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。

Trademark Information

Contents

Chapter 5 User Logins and Persistence

Chapter 6 Grouping

Chapter 7 Licensing

Chapter 8 Zoning

Chapter 10 Security Management

Chapter 11 Call Home

Chapter 12 Firmware Download

Chapter 13 ISL Checking

Figures

Tables

Preface

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of the EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B. Therefore, some functions described in this guide may not be supported by all versions of EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B currently in use. For the most up-to-date information on product features, see the product release notes.

If an EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance. For other Brocade-based products, please contact your switch supplier.

Audience

This guide is intended for use by system administrators during installation and configuration of the DS-16B2, DS-32B2, and ED-12000B switches as well as Brocade-based products from other suppliers.

Readers of this guide are expected to be familiar with Brocade-based switch products and their operating environment including the EMC Connectrix Departmental Switch DS-16B2, DS-32B2, and Enterprise Director ED-12000B.

Organization

This manual provides the following information about Fabric Manager:

Chapter 1, *Introduction*, introduces the Connectrix B Fabric Manager, its system requirements, advantages, and highlights, along with terms and concepts.

Chapter 2, *Installing Fabric Manager*, provides information on installing, launching, registering, and uninstalling Fabric Manager.

Chapter 3, *Fabric Manager Interface*, discusses the Fabric Manager basic GUI, identifies many of the visual elements when Fabric Manager is opened, and focuses on icons that appear in Summary view.

Chapter 4, *Common Fabric Manager Tasks*, explains how to perform common Fabric Manager tasks.

Chapter 5, *User Logins and Persistence*, discusses logging in to use the software, the data that persists, and persistence files.

Chapter 6, *Grouping*, explains how to create, delete, export, and import a group.

Chapter 7, *Licensing*, shows how to import and export license keys, remove a license key from a switch, and perform e-licensing.

Chapter 8, *Zoning*, provides high-level zoning instructions and details about zoning concepts and practices.

Chapter 9, *Fabric Watch*, explains Fabric Watch terms, how it works, how to use and access Fabric Watch, how to view Fabric Watch alarms, configuring threshold boundaries and alarms and e-mail alert, how to enable and disable thresholds, and how to configure threshold traits and view an alarm configuration report.

Chapter 11, *Call Home*, describes CallHome and shows how to configure CallHome, edit configurations, and globally enable or disable CallHome.

Chapter 10, *Security Management*, explains how to access, configure, and manage security using the Fabric Manager GUI.

Chapter 12, *Firmware Download*, discusses how to perform a firmware download to multiple switches.

Chapter 13, *ISL Checking*, explains how to use Interswitch Link (ISL) checking to monitor any changes to your ISL topology.

Chapter 14, *Fabric Checking*, shows how you can configure the Fabric Checkin feature to monitor the fabric and register events when you add switches to, or remove switches from, the fabric.

Chapter 15, *Fabric Merge Check*, explains how to check fabrics.

Chapter 16, *Comparing Configurations*, contains information on how to save a baseline configuration to a file, compare switches to a baseline, and customize baseline templates.

Chapter 17, *Complete Fabric Backup and Compare*, explains how to back up a fabric and compare a fabric to a backup.

Chapter 18, *Sequenced Reboot*, shows how to create a reboot group and perform a sequenced reboot.

Chapter 19, *Emulex HBA Firmware Download*, gives steps to download firmware to one or more HBA.

Chapter 20, *Troubleshooting*, provides solutions to problems that you may encounter as you manage your SAN with Fabric Manager.

Appendix A, *File Menu Reference*, provides information on File menu options.

Appendix B, *Edit Menu Reference*, describes the options in the Edit menu.

Appendix C, *View Menu Reference*, describes the various Fabric Manager views.

Appendix D, *Actions Menu*, provides information on fabric, switch, and port actions.

Appendix E, *Topology Menu Reference*, shows options that can be accessed from the Topology menu.

Appendix F, *Tools Menu Reference*, discuses the Tools menu options and reboot, config, and licensing sub-menus.

Appendix G, *Help Menu Reference*, provides information on the Help menu.

Appendix H, *Zoning Reference*, describes information about zoning fields and components of the Zone Administration window components.

Appendix I, *Fabric Watch Reference*, discusses the Alarm Notification, Threshold Configuration, and E-Mail Configuration tabs.

Appendix J, *CallHome External Executable Reference*, explains CallHome executable requirements.

Appendix K, *Customer Support*, provides information on contacting EMC Customer Support.

The *Glossary* provides terms used in this document.

- security (ENABLED by default)

  secmodeshow
  secstatsshow
  secfabricshow

- network (ENABLED by default)

  bootenv
  sin
  df
  ifconfig
  route
  hostname

- portlog (ENABLED by default)

  portlogdump

- system (ENABLED by default)

  myid
  version
  firmwareshow
  uptime
  switchstatushow
  switchshow
  hadump (includes hashow, ipaddrshow)
  tempshow
  sensorshow
  psshow
  licenseshow
  portflagsshow
  portcfgshow
  porterrshow
  fwsamshow
  agtcfgshow
  slotshow (product-dependent)
  fwalarmsfiltershow
  chassisshow
  timeout
  historyshow
  configshow

- extend (DISABLED by default)

mii-tool
du
ps
rpm
dmesg
fstab
mtab
various proc entries
find core files

- exception (ENABLED by default)

  errdump

- port (ENABLED by default)

  diagshow (per-slot)
  portshow (per-slot)
  portloginshow (per-slot)
  portregshow (per-slot)
  portrouteshow (per-slot)

- fabric (ENABLED by default)

  fabricshow
  islshow
  trunkshow
  topologyshow
  fabstateshow
  fabswitchshow
  fabportshow
  fspfshow
  fcplogshow
  zone-stateshow
  portcamshow
  cfgsize
  cfgshow
  rcssmshow
  rcsinfoshow
  rcsregistryshow

- services (ENABLED by default)

  nsshow
  nsallshow
  nscamshow
  fdmishow
  dmicacheshow

`-ports itemlist` Specify a list of user ports to test. By default all the user ports in the current slot will be assumed. See itemlist help pages for further details.

Example **To stop the porttest command:**

```
switch:admin> stopporttest
```

See Also

```
porttest
porttestshow
loopporttest
fporttest
crossporttest
portloopbacktest
spinfab
```

supportshow

Print switch information for debugging purposes.

Syntax For a ED-12000B:

`supportshow [slotnumber[/port1-port2]] [lines]`

For a DS-32B2:

`supportshow [port1-port2] [lines]`

Availability All users.

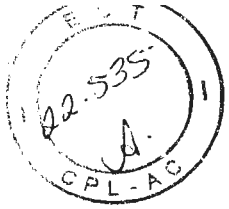
Description Use this command to display support information from groups of pre-selected Fabric OS and LINUX commands. You can specify the range of ports for which this information is display.

The output from this command can be very long.

These commands are organization by groups, but note that the order of the groups listed below is not the same as executed by the command.

The commands have been arranged in groups identified as follows:

- OS (ENABLED by default) - LINUX commands are not documted in this manual.



`-ports itemlist` Specify a list of user ports to run the test. If omitted, all the user ports in the switch will be assumed. Refer to `itemlist` for more information about selecting ports. This operand is optional.

Example **To run a statistics counter test on a switch:**

```
switch:admin> statstest -passcnt 1 -ports 1/0-15
Running Statistics Counter Test ....... passed.
switch:admin>
```

Errors When it detects failure(s), the subtest may report one or more of the following error messages:

```
DIAG-STSINIT
DIAG-STSNULL
DIAG-STSSID
DIAG-STSXMIT
DIAG-STSRCV
DIAG-STSFRMCNT
DIAG-STSWRDCNT
DIAG-STSALPACNT
```

See Also

```
portregtest
centralmemorytest
cmitest
sramretentiontest
turboramtest
camtest
filtertest
portloopbacktest
spinsilk
```

stopporttest

Terminate the running **porttest**.

Syntax `stopporttest [-ports itemlist]`

Availability Admin

Description Use this command to stop the currently running `porttest`. Refer to the `porttest` command for more information. If `porttest` is running on a non-singlemode, use `stopporttest` to stop the test.

Operands This command has the following operand:

```
cmitest
turboramtest
filtertest
portloopbacktest
spinsilk
```

statstest

Run a statistics counter diagnostic test.

Syntax `statstest [-passcnt count][-ports itemlist]`

Availability Admin

Description Use this command to verify the 2 Gbit/sec ASIC statistics counter logic. It can run on every base port of quadrant, and send the frame through internal loopback with no CRC data to induce the CRC error. This command is also run from `camtest`.

This test covers following statistics counter functionality.

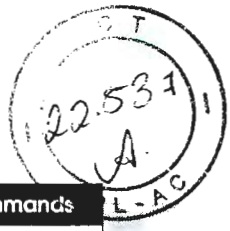
1. The number of received frames with CRC error that matched the SID-DID pair specified in the LINK table. There are a total 16 of these statistics counters (0-15), respectively.
2. The number of received words in frames that matched the SID-DID pair specified in the LINK table. There are a total 16 of these statistics counters (0-15), respectively.
3. The number of transmitted words in frames that matched the SID-DID pair specified in the LINK table. There are a total 16 of these statistics counters (0-15), respectively.
4. The number of frames with CRC error that matched the corresponding ALI (0-127), respectively.

This command may not be executed on an operational switch. You must first disable the switch using the `switchdisable` command.

There is a LINK table that stores 16 pairs of SID-DID address. Each of the SID-DID pair is named a LINK. This table is used for gathering statistics that match the LINK.

Operands This command has the following operands:

`-passcnt count` Specify the number of times to perform this test. The default value is 1. This operand is optional.



```
0xffffffff
0x55555555
0x33333333
0x0f0f0f0f0f
```

For details about the patterns used in diagnostic tests, refer to the `datatypeshow` command.

The `sramretentiontest` command may not be executed on an operational switch. You must first disable the switch using the `switchdisable` command.

Operands This command has the following operand:

`-slot` *number*	Specify the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is set to 0 and designed to operate on fixed port count products.
`-passcnt` *count*	Specify the number of times to execute this test. The default value is 1.<q> to stop
`-ports` *itemlist*	Specify a list of blade ports to test. By default all the blade ports in the specified slot will be used. See `itemlist` for more details.
`-skip` *bitmask*	Specify a patterns to skip in the test. This command will use the data patterns described above by default. Using this option, the user can intentionally skip one or more pattern(s) if needed.
`-delay` *value*	Specify the delay between the read and write in seconds. The default value is 10, which is 10 seconds.

Example **To run a data retention test:**

```
switch:admin> sramretentiontest
Running SRAM Retention Test ... passed.
```

Errors Below are the possible error messages if failures are detected:

```
BUS_TIMEOUT
REGERR
REGERR_UNRST
```

See Also

```
portregtest
centralmemorytest
```

```
LESSN_STATUS_ERR
MBUF_STATE_ERR
MBUF_STATUS_ERRBAR>
NO_SEGMENT
PORT_ABSENT
PORT_DIED
PORT_ENABLE
PORT_M2M
PORT_STOPPED
PORT_WRONG
RXQ_FRAME_ERR
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FRX
STATS_FTX
TIMEOUT
XMIT
```

See Also

```
backport
camtest
centralmemorytest
cmemretentiontest
cmitest
crossporttest
itemlist
portloopbacktest
portregtest
spinjitter
sramretentiontest
```

sramretentiontest

Data retention test of the miscellaneous SRAMs in ASIC.

Syntax

`sramretentiontest [-slot` *number*`] [-passcnt` *count*`] [-ports` *itemlist*`] [-skip` *bitmask*`] [-delay` *value*`]`

Availability

Admin

Description

Use this command to verify that data written into the miscellaneous SRAMs in the ASIC are retained after a 10 second wait. The method used is to write a fill pattern to all SRAMs, wait 10 seconds, and then read all SRAMs, checking that the data read matches the data previously written. Then the test is repeated using the inverted version of the pattern. The test will use four QUAD_FILL patterns and one QUAD_RAMP pattern with random seed. The first four QUAD_FILL patterns are:

Example To run spinsilk on a switch:

```
switch:admin> spinsilk -ports 1/0 - 1/2
Running Spin Silk .............
One moment please ...Ports Segmented (0)
switchName:     switch
switchType:     10.1
switchState:    Offline
switchRole:     Disabled
switchDomain:   1 (unconfirmed)
switchId:       fffc01
switchWwn:      10:00:00:60:69:80:03:0c
switchBeacon:   OFF
blade1: Beacon: OFF
blade2: Beacon: OFF
blade3: Beacon: OFF
blade4: Beacon: OFF

Area Slot Port Gbic Speed State
=====================================
  0    1    0   id    2G   Online    Testing  ......
  1    1    1   id    2G   Online    Testing  ......
  2    1    2   id    2G   Online    Testing  ......
<output truncated>
```

Errors Below are the possible error messages if failures are detected:

```
DATA
EPI1_STATUS_ERR
ERR_STAT
ERR_STATS
ERR_STATS_2LONG
ERR_STATS_BADEOF
ERR_STATS_BADOS
ERR_STATS_C3DISC
ERR_STATS_CRC
ERR_STATS_ENCIN
ERR_STATS_ENCOUT
ERR_STATS_TRUNC
ERR_STAT_2LONG
ERR_STAT_BADEOF
ERR_STAT_BADOS
ERR_STAT_C3DISC
ERR_STAT_CRC
ERR_STAT_ENCIN
ERR_STAT_ENCOUT
ERR_STAT_TRUNC
FDET_PERR
FINISH_MSG_ERR
FTPRT_STATUS_ERR
INIT
```

For `lbMode = 0, 1` the following speed modes are available to test the speed negotiation:

- 3: set all even ports' speed for auto-negotiate, set all odd ports' speed for 1 Gbit/sec.
- 4: set all even ports' speed for auto-negotiate, set all odd ports' speed for 2 Gbit/sec.
- 5: set all odd ports' speed for auto-negotiate, set all even ports' speed for 1 Gbit/sec.
- 6: set all odd ports' speed for auto-negotiate, set all even ports' speed for 2 Gbit/sec.

For `lbMode = 2, 3` the following speed modes are available to test fifo underrun.

- 3,5: set all even ports' speed for 2 Gbit/sec, set all odd ports' speed for 1 Gbit/sec.
- 4,6: set all even ports' speed for 1 Gbit/sec, set all odd ports' speed for 2 Gbit/sec.

`-verbose` *mode* — Specify a non-zero value, to display more detailed information during the test. This mode should be used for debugging purpose. This operand is optional.

`-ports` *itemlist* — Specify a list of user ports to test. By default all of the user ports in the current switch are tested. This option may be used to restrict testing to the specified ports.

The state of the GBIC mode is saved in non-volatile memory and remains active over a reboot until it is disabled as follows:

```
switch:admin> setsfpmode 0
```

Prior to running this command make sure you disable the switch, set the GBIC mode to 1, and install loopback cables on all GBIC ports you want to test.

Because this test includes the GBIC and the fiber cable in its test path, use the results from this test in conjunction with the results from `crossporttest` and `portloopbacktest` to determine those switch components are not functioning properly.

Operands

This command has the following operands:

`-nmegs` *count*
: Specify the number of million frames to send. The test will progress until the specified number of frames has been transmitted on each port. The default value is 10, so the number of frames sent will be at least 10 million.

`-lb_mode` *mode*
: Specify the loopback point for the test. By default, `spinsilk` uses loopback plugs as described above. However for debug purposes you can select other loopback modes as follows:

  0: Cable Loopback.

  1: Port Loopback (loopback plugs).

  2: External (SERDES) loopback.

  3: Silkscreen loopback.

  4: Serial link wrapback.

  5: Internal (parallel) loopback.

`-spd_mode` *mode*
: Specify the speed mode for the test. For 1 Gbit/sec only products it is ignored. The exact operation of modes 3 through 6 depends upon the loopback mode selected. When speed modes 3 through 6 are used with cables, they must be connected EVEN to ODD or the test will fail.

  - 0: set all ports' speed for auto-negotiate.
  - 1: set all ports' speed to lock at 1 Gbit/sec.
  - 2: set all port's speed to lock at 2 Gbit/sec.

LoopBack Mode

There are four loopback modes that can be used when executing the `spinsilk` command. The modes are specified by entering:

- `0` for cable mode. This loopback mode is the default mode and tests only `M->N` connections. It requires that the user connect a cable from one port to a different port.
- `1` for single port also loopback mode. This lb_mode tests `M->N` and `M->M` connections.

  If `M->N` cable connections are used the `spinsilk` command operates identically in `lb_mode 0` and `lb_mode 1`.

  If `M->M` loopback plugs are used with SPLB mode disabled the `spinsilk` command will circulate frames between pairs of `M->M` connected ports as follows:

  `P1 TX >>> P1 RX -> P2 TX >>> P2 RX -> P1 TX`
  where:

  `>>>` is a cable or internal loopback

  `->` is a routing table entry

  The connections between pairs of `M->M` ports are chosen to exercise the connections between as many ASICs as possible subject to the availability of pairs of `M->M` ports.

  In mode `1` with SPLB mode disabled the `spinsilk` command only circulates frames within each single port and none of the ASIC to ASIC connections are tested. This mode should only be used for fault isolation.
- `2` for external loopback mode. The external loopback test creates a test loop between two ports on different ASICs and also tests the Serializer Deserializer functionality.
- `5` for internal loopback mode. The internal loopback test creates a test loop between two ports on a single ASIC.

Refer to the `setsplbmode` command for more information on how the loopback mode setting changes the execution of this command.

GBIC/SFP Mode

If the `spinsilk` command is executed with GBIC mode activated, only ports containing GBICs are tested. To activate GBIC mode, execute the following command prior to executing the `spinsilk` command:

```
switch:admin> setsfpmode 1
```

partner port N through an external fiber cable, exercising all the switch components.

The `spinsilk` command may not be executed on an operational switch. You must first disable the switch using the `switchdisable` command.

The cables can be connected to any port combination with the condition that the cables and SFPs connected are of the same technology. For example, a short wavelength SFP port must be connected to another short wavelength SFP port through a short wavelength cable; or a long wavelength port must be connected to another long wavelength port.

Optimum test coverage occurs with lb_mode 1, `M->M` loopback plugs and `splbmode` disabled. In this case every port will exchange frames with every other port and all of the ASIC to ASIC connections are tested.

The frames are continuously transmitted and received in all ports in parallel. The port LEDs flicker green rapidly while the test is running.

At each pass, the frame is created from a different data type. There are seven data types:

1. CSPAT: 0x7e, 0x7e, 0x7e, 0x7e, ...
2. BYTE_LFSR: 0x69, 0x01, 0x02, 0x05, ...
3. CHALF_SQ: 0x4a, 0x4a, 0x4a, 0x4a, ...
4. QUAD_NOT: 0x00, 0xff, 0x00, 0xff, ...
5. CQTR_SQ: 0x78, 0x78, 0x78, 0x78, ...
6. CRPAT: 0xbc, 0xbc, 0x23, 0x47, ...
7. RANDOM: 0x25, 0x7f, 0x6e, 0x9a, ...

If seven passes are requested, the seven different data types are used in the test. If eight passes are requested, the first seven frames use unique data types, and the eighth is the same as the first.

spinSilk Modes

These are the test modes. These modes can be used together to test specific ports.

- Loopback mode
- SFP mode

```
ERR_STAT_BADOS
ERR_STAT_C3DISC
ERR_STAT_CRC
ERR_STAT_ENCIN
ERR_STAT_ENCOUT
ERR_STAT_TRUNC
FINISH_MSG_ERR
INIT
MBUF_STATE_ERR
NO_SEGMENT
PORT_ABSENT
PORT_DIED
PORT_ENABLE
PORT_M2M
PORT_STOPPED
PORT_WRONG
RXQ_RAM_PERR
STATS
STATS_C3FRX
STATS_FRX
STATS_FTX
TIMEOUT
XMIT
```

See Also

```
camtest
centralmemorytest
cmemretentiontest
cmitest
crossporttest
itemlist
portloopbacktest
spinsilk
sramretentiontest
```

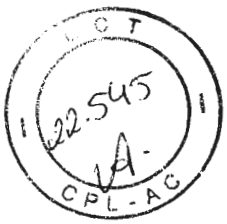
spinsilk

Functional test of internal and external transmit and receive paths at full speed.

Syntax `spinsilk [-nmegs` *count*`] [-lb_mode` *mode*`] [-spi_mode` *mode*`] [-verbose` *mode*`] [-ports` *itemlist*`]`

Availability Admin

Description This command verifies the functional operation of the switch by setting up the routing hardware such that frames received by port M are retransmitted through port N. Likewise frames received by port N are retransmitted through port M. Each port M sends 1 frame to its



`-setfail` *mode* — This parameter may be used to instruct `spinfab` how to mark failed ports. If set to 1, it will mark failing ports as FAILED. If set to 0, it will not mark failed ports as FAILED. It is to minimize the impact on live fabrics. This test normally logs errors but does not set the port status to FAILED. This parameter is provided to force the failing ports to be marked as FAILED in the same manner as other diagnostics. In test or qualification environments without live traffic, this may be useful with large values of `-nmegs` count. This mode is disabled by default.

`-domain` *value* — This parameter is used to specify a specific remote domain that the switch is connected to. The default is to automatically determine the remote domain number. This may not work properly in certain conditions.

Example **To test cascading ISL links:**

```
switch:admin> spinfab -ports 1/0 - 1/2
spinfab running...
spinfab: Completed 11 megs, status:  passed.
        port 0 test status: 0x00000000 --  passed.
        port 1 test status: 0x00000000 --  passed.
        port 2 test status: 0x00000000 --  passed.
Test Complete: "spinfab" Pass 10 of 10
Duration 0 hr, 0 min & 41 sec (0:0:41:877).
passed.
switch:admin>
```

Errors When it detects failure(s), the test may report one or more of the following error messages:

```
DATA
ERR_STAT
ERR_STATS
ERR_STATS_2LONG
ERR_STATS_BADEOF
ERR_STATS_BADOS
ERR_STATS_C3DISC
ERR_STATS_CRC
ERR_STATS_ENCIN
ERR_STATS_ENCOUT
ERR_STATS_TRUNC
ERR_STAT_2LONG
ERR_STAT_BADEOF
```

then sent to the neighbor port attached to each active E_port specified. Since the default action for such frames (which never occur for normal traffic) is to route them back to the sender, the frames that are sent in this manner will circulate until the test stops them.

The frames are continuously transmitted and received in all ports in parallel. The port LEDs flicker green rapidly while the test is running. While the frames are circulating the RX frame count and port CRC and encoder error statistics will be monitored and errors will be generated if a port stops or a low level error occurs. Every one million frames the circulating frames will be captured to verify that they are still circulating and that they are still in-order. In this manner the entire path to the remote switch may be verified as well as the proper in-order delivery operation of any trunk groups present.

The switch will remain in normal operation while this test is running, however some performance degradation will occur due to the ISL links being saturated with test frames. Because of this you should use caution when running this test on live fabrics, consider only testing one trunk group or ISL link at a time, and do not run the tests for extended periods of time.

This test is best combined with the online `crossporttest` for ISL link failure isolation. If this test fails, replace the cable with a loop-back plug and run `crossporttest` to verify the local switch and media. If these pass then the fault lies in the cable or remote switch/media.

The frames are continuously transmitted and received in all ports in parallel. The port LEDs flicker green rapidly while the test is running.

Operands This command has the following operands:

`-nmegs` *`count`* Specify the number of frames to send in millions. The test will progress until the specified number of frames has been transmitted on each port. The default value is 10, that is, 10 million frames. This command only approximately counts the frames and the actual number of frames sent will be slightly larger, particularly at 2 Gbit/sec link speeds.

`-ports` *`itemlist`* Specify a list user ports to test. By default, all of the ISL ports in the current switch will be tested. See itemlist help pages for further details.

FA-TRAP	Specifying yes means the SNMP management application can receive FA-TRAPS from the switch. The default value is yes.
SW-EXTTRAP	Specifying yes means the SNMP management application can receive SW-EXTTRAPS from the switch. The default value is yes.
HA-TRAP	Specifying yes means the SNMP management application can receive HA-TRAPS from the switch. The default value is yes.

Operands None

Example **To view or modify the options for configuring SNMP MIB traps:**

```
switch:admin> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
FE-MIB SW-MIB FA-MIB FICON-MIB HA-MIB SW-TRAP FA-TRAP FICON-TRAP HA-TRAP
FA-MIB (yes, y, no, n): [yes]
FICON-MIB (yes, y, no, n): [yes]
HA-MIB (yes, y, no, n): [yes]
SW-TRAP (yes, y, no, n): [yes]
FA-TRAP (yes, y, no, n): [yes]
SW-EXTTRAP (yes, y, no, n): [no] y
FICON-TRAP (yes, y, no, n): [yes]
HA-TRAP (yes, y, no, n): [yes]
switch:admin>
```

See Also `agtcfgshow`
`agtcfgset`
`agtcfgdefault`

spinfab

Test for Cascaded switch ISL links.

Syntax `spinfab [-nmegs` *`count`*`] [-ports` *`itemlist`*`] [-setfail` *`mode`*`] [-domain` *`value`*`]`

Availability Admin

Description Use this command to verify the intended functional operation of the ISL links between switches at the maximum speed of 2 Gbit/sec by setting up the routing hardware such that test frames received by each E_port retransmitted on the same E_port. Several frames are

Example To display a blade inventory and status:

```
switch:admin> slotshow
Slot   Blade Type    ID     Status
---------------------------------
1      SW BLADE      2      FAULTY
2      SW BLADE      2      DISABLED
3      SW BLADE      2      ENABLED
4      SW BLADE      2      DIAG RUNNING POST2
5      CP BLADE      1      ENABLED
6      CP BLADE      1      ENABLED
7      UNKNOWN              VACANT
8      SW BLADE      2      DIAG RUNNING POST1
9      SW BLADE      2      INSERTED, NOT POWERED ON
10     UNKNOWN              VACANT
```

See Also
```
chassisshow
sloton
slotoff
slotpoweron
slotpoweroff
```

snmpmibcapset

View and modify options for configuring SNMP MIB trap capability.

Syntax `snmpmibcapset`

Availability Admin

Description This command enables a user to turn on or off certain MIBS and TRAPS. This command also enables a user to turn on or off group information and SSN in SW trap messages. It first displays current settings and then prompts the user to change the values for each parameter.

FA-MIB	Specifying yes means the user can access FA-MIB variables with an SNMP manager. The default value is yes.
HA-MIB	Specifying yes means the user can access HA-MIB variables with an SNMP manager. The default value is yes.
SW-TRAP	Specifying yes means the SNMP management application can receive SW-TRAPS from the switch. The default value is yes.

four fields for each slot. This command is only supported on the ED-12000B. The fields and their possible values are as follows:

Slot — Displays the physical slot number.

Blade Type — Displays the blade type:

- SW BLADE
  The blade is a Switch.
- CP BLADE
  The blade is a Control Processor.
- UNKNOWN
  Blade not present or its type is not recognized.

ID — Displays the hardware ID of the blade type.

- 1 represents a CP BLADE
- 2 represents a SW BLADE

Status — Displays the status of the blade:

- VACANT
  The slot is empty.
- INSERTED, NOT POWERED ON
  The blade is present in the slot but is turned off.
- DIAG RUNNING POST1
  The blade is present, powered on, and running the post initialization power on self tests.
- DIAG RUNNING POST2
  The blade is present, powered on, and running the POST (power on self tests).
- ENABLED
  The blade is on and enabled.
- DISABLED
  The blade is powered on but disabled.
- FAULTY
  The blade is faulty because an error was detected.
- UNKNOWN
  The blade is inserted but its state cannot be determined.

Operands None

slot	Specify the physical slot number of the blade to be powered down. This operand is required.

Example **To power off blade unit 3:**

```
switch:admin> slotpoweroff 3
Slot 3 is being powered off
```

See Also

```
slotshow
slotpoweron
```

slotpoweron

Power on a blade unit.

Syntax `slotpoweron slot`

Availability Admin

Description Use this command to turn on the power to a blade unit. The slot must have a valid blade unit present and the blade unit must be currently powered off.

Operands This command has the following operands:

slot	Specify the physical slot number of the blade to be powered on. This operand is required.

Example **To power on blade unit 3:**

```
switch:admin> slotpoweron 3
Powering on slot 3.
```

See Also

```
slotshow
slotpoweroff
```

slotshow

Display slot status.

Syntax `slotshow`

Availability All users

Description Use this command to inventory and display the current status of each slot in the system. The format of the display includes a header and

Example **To power off blade unit 3:**

```
switch:admin> slotoff 3
Slot 3 is being disabled.
```

See Also

```
slotshow
sloton
```

sloton

Enable a blade slot.

Syntax `sloton slot`

Availability Admin

Description Use this command to re-enable a blade unit that was previously disabled.

Operands This command has the following operands:

slot	Specify the physical slot number of the blade to be enabled. This operand is required.

Example **To power off blade unit 3:**

```
switch:admin> sloton 3
Slot 3 is being enabled.
```

See Also

```
slotshow
slotoff
```

slotpoweroff

Power off a blade unit.

Syntax `slotpoweroff slot`

Availability Admin

Description Use this command to turn off the power to a blade unit. The slot must have a valid blade unit present and the blade unit must be of a type that can be powered off.

Operands This command has the following operands:

See Also `shellflowcontrolenable`

shellflowcontrolenable

Disables XON/XOFF flow control to the shell task.

Syntax `shellflowcontrolenable`

Availability Admin

Description Use this command to enable XON/XOFF flow control to the shell task. Disabling XON/XOFF flow control is the recommended behavior for the switch, however, if it becomes necessary to enable XON/XOFF flow control, it may be done with this command. Flow control will be enabled for both serial port and telnet access into the command shell.

Once enabled, even in the event of a power failure, the switch will boot up with XON/XOFF flow control ENABLED.

Operands None

Example **To enable flow control:**

```
switch:admin> shellflowcontrolenable
Committing configuration...done.
```

See Also `shellflowcontroldisable`

slotoff

Disable a blade slot.

Syntax `slotoff` *`slot`*

Availability Admin

Description Use this command to disable a non-faulty blade unit while leaving the blade unit powered on.

Operands This command has the following operands:

`slot`	Specify the physical slot number of the blade to be disabled. This operand is required.

This example shows detailed SFP information for a ED-12000B:

```
switch:admin> sfpshow 1/3
Identifier:  3    SFP
Connector:   7    LC
Transceiver: 050c402000000000 100,200_MB/s M5,M6 sw Inter_dist
Encoding:    1    8B10B
Baud Rate:   21   (units 100 megabaud)
Length 9u:   0    (units 100 meters)
Length 50u:  30   (units 10 meters)
Length 625u: 13   (units 10 meters)
Length Cu:   0    (units 1 meter)
Vendor Name: FINISAR CORP.
Vendor OUI:  00:90:65
Vendor PN:   FTRJ-8519-3-2.5
Vendor Rev:  X1
Options:     0012 Loss_of_Sig,Tx_Disable
BR Max:      0
BR Min:      0
Serial No:   H112YFR
Date Code:   010418
switch:admin>
```

See Also `switchshow`

shellflowcontroldisable

Disables XON/XOFF flow control to the shell task.

Syntax `shellflowcontroldisable`

Availability Admin

Description Use this command to disable XON/XOFF flow control to the shell task. Disabling XON/XOFF flow control is the recommended behavior for the switch. Flow control will be disabled for both serial port and telnet access into the command shell.

Once disabled, even in the event of a power failure, the switch will boot up with XON/XOFF flow control DISABLED.

Operands None

Example **To disable flow control:**

```
switch:admin> shellflowcontroldisable
Committing configuration...done.
```

Example The example below shows SFP summary information followed by detailed information for an SFP:

```
switch:admin> sfpshow
Area  0: id (sw) Vendor: AGILENT          Serial No: A00149567
Area  1: id (sw) Vendor: AGILENT          Serial No: A00108650
Area  2: id (sw) Vendor: AGILENT          Serial No: A00149568
Area  3: id (sw) Vendor: AGILENT          Serial No: A00108567
Area  4: id (sw) Vendor: AGILENT          Serial No: A00152395
Area  5: id (sw) Vendor: AGILENT          Serial No: A00149623
Area  6: id (sw) Vendor: AGILENT          Serial No: A00152423
Area  7: id (sw) Vendor: AGILENT          Serial No: A00108932
Area  8: id (sw) Vendor: AGILENT          Serial No: A00111165
Area  9: id (sw) Vendor: AGILENT          Serial No: A00079899
Area 10: id (sw) Vendor: AGILENT          Serial No: A00079319
Area 11: id (sw) Vendor: AGILENT          Serial No: A00079917
Area 12: id (sw) Vendor: AGILENT          Serial No: A00079274
Area 13: id (sw) Vendor: AGILENT          Serial No: A00079348
Area 14: id (sw) Vendor: AGILENT          Serial No: A00079843
Area 15: id (sw) Vendor: AGILENT          Serial No: A00150114
Area 16: id (sw) Vendor: AGILENT          Serial No: A00079337
Area 17: id (sw) Vendor: AGILENT          Serial No: A00148599
Area 18: id (sw) Vendor: AGILENT          Serial No: A00079856
Area 19: id (sw) Vendor: AGILENT          Serial No: A00079937
Area 20: id (sw) Vendor: AGILENT          Serial No: A00079832
Area 21: id (sw) Vendor: AGILENT          Serial No: A00079835
Area 22: id (sw) Vendor: AGILENT          Serial No: A00079332
Area 23: id (sw) Vendor: AGILENT          Serial No: A00079852
Area 24: id (sw) Vendor: AGILENT          Serial No: A00148593
Area 25: id (sw) Vendor: AGILENT          Serial No: A00084645
Area 26: id (sw) Vendor: AGILENT          Serial No: A00079381
Area 27: id (sw) Vendor: AGILENT          Serial No: A00084644
Area 28: id (sw) Vendor: AGILENT          Serial No: A00084654
Area 29: id (sw) Vendor: AGILENT          Serial No: A00079318
Area 30: id (sw) Vendor: AGILENT          Serial No: A00079848
Area 31: id (sw) Vendor: AGILENT          Serial No: A00079356
switch:admin>
```

extended information that describes the SFPs capabilities, interfaces, manufacturer, and other information.

SFPs are polled by a background process. The `sfpshow` command retrieves the latest information from cache. The cache values for each SFP are updated when the SFP is hot plugged, when it is removed, or when the Fabric OS polls the SFPs. In the ED-12000B, if there is a lot of activity on the switch, poll updates may take several minutes.

Use this command with no operand to display a summary of all SFPs in the switch. The summary shows the SFP type (see `switchshow` for an explanation of the two letter codes) and, for Serial ID SFP, the vendor name and SFP serial number.

Use this command with the slot and portnumber operand to display detailed information about the Serial ID SFP in that port.

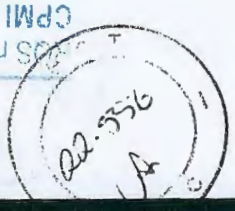
For Finisar `smart` SFPs, five additional fields are displayed: module temperature, voltage, received optical power, transmitted optical power (longwave only), and laser diode drive current.

Operands This command has the following operand:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

`portnumber` Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.



Example To enable or disable a two port loopback:

```
switch:admin> setsplbmode 1
Config update Succeed.
SPLB mode is now 1 (Enabled).
switch:admin> setSplbMode 0
Config update Succeed.
SPLB mode is now 0 (disabled).
```

See Also `setsfpmode`
`spinsilk`

setverbose

Set verbose level of the module to specified level.

Syntax `setverbose module_name, level`

Availability Admin

Description Use this command to set the verbose level of the specified module.

Operands This command has the following operands:

module_name	Specify the name of the module for which verbose level is to be set.
level	Specify the verbose level to be set for the specified module.

Example The following example shows how to set the verbose level of module named NS to value 3:

```
switch:admin> setverbose NS 3
```

See Also `dbgshow`

sfpshow

Display serial ID SFP information.

Syntax `sfpshow [slotnumber/] [portnumber]`

Availability All users

Description Use this command to display information about Serial Identification SFPs (also known as module definition 4 SFPs). These SFPs provide

setsplbmode

Enable or disable two port loopback.

Syntax `setsplbmode [mode | -show]`

Availability Admin

Description Use this command to enable or disable SPLB mode. The mode is saved in non-volatile memory and stays in that mode until the next execution of `setSplbMode`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

The SPLB mode, when enabled, forces the `spinsilk` command to disable two port loopback for `M->M` connected ports. This may be useful to isolate internal switch problems from SFP problems since the internal paths are used much less with SPLB mode enabled.

The SPLB mode, when disabled, forces the `spinsilk` command to circulate frames between pairs of `M->M` connected ports as follows:

```
P1 TX >>> P1 RX -> P2 TX >>> P2 RX -> P1 TX
```

where:

`>>>` is a cable or internal loopback

`->` is a routing table entry

The connections between pairs of `M->M` ports will be chosen to exercise the connections between as many chips (or bloom quadrants) as possible subject to the setting of allow_intra_chip and the availability of pairs of `M->M` ports.

Any ports that are cross-cabled will be routed to each other in the normal manner regardless of the setting of SPLB mode:

```
P1 TX >>> P2 RX -> P1 TX
   P2 TX >>> P1 RX -> P2 TX
```

Operands This command has the following operands:

mode	Specify 1 to enable SPLB mode or 0 to disable SPLB mode. If no mode is specified the current value is displayed. This operand is optional.
`-show`	Specify the `-show` operand to display the current setting. This operand is optional.

setsfpmode

Enable or disable media mode.

Syntax

```
setmediamode [mode | -show]
setgbicmode [mode | -show]
setsfpmode [mode | -show]
```

Availability

Admin

Description

Use these commands to enable media mode (GBIC or SFP) if the mode value is non-zero and disable the media mode if the mode value is 0. The mode is saved in flash memory and stays in that mode until the next execution of `setmediamode`, `setsfpmode`, or `setgbicmode`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Media mode when enabled modifies the behavior of the diagnostic test methods so that ports without media installed are not tested. Normally tests such as `crossporttest` or `spinsilk` will fail if any port is not operating properly, but with media mode enabled the functional tests will be skipped on ports that do not contain media.

Operands

This command has the following operands:

mode	Specify 1 to enable media mode or 0 to disable media mode. If no mode is specified the current value is displayed. Any other value will enable media mode.
`-show`	Specify the *-show* operand to display the current setting. This operand is optional.

Example

To enable or disable media mode:

```
switch:admin> setgbicmode 1
GBIC mode is now 1 (Enabled).
switch:admin> setsfpmode 0
SFP mode is now 0 (disabled).
switch:admin> setmediamode -show
Media mode is now 0 (disabled).
```

See Also

```
crossporttest
itemlist
spinjitter
spinsilk
```

setmediamode

Enable or disable media mode.

Syntax

```
setmediamode [mode | -show]
setgbicmode [mode | -show]
setsfpmode [mode | -show]
```

Availability

Admin

Description

Use these commands to enable media mode (GBIC or SFP) if the mode value is non-zero and disable the media mode if the mode value is 0. The mode is saved in flash memory and stays in that mode until the next execution of `setmediamode`, `setsfpmode`, or `setgbicmode`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Media mode when enabled modifies the behavior of the diagnostic test methods so that ports without media installed are not tested. Normally tests such as `crossporttest` or `spinsilk` will fail if any port is not operating properly, but with media mode enabled the functional tests will be skipped on ports that do not contain media.

Operands

This command has the following operands:

mode	Specify 1 to enable media mode or 0 to disable media mode. If no mode is specified the current value is displayed. Any other value will enable media mode.
`-show`	Specify the `-show` operand to display the current setting. This operand is optional.

Example

To enable or disable media mode:

```
switch:admin> setgbicmode 1
GBIC mode is now 1 (Enabled).
switch:admin> setsfpmode 0
SFP mode is now 0 (disabled).
switch:admin> setmediamode -show
Media mode is now 0 (disabled).
```

See Also

```
crossporttest
itemlist
spinjitter
spinsilk
```

setgbicmode

Enable or disable media mode.

Syntax

```
setmediamode [mode | -show]
setgbicmode [mode | -show]
setsfpmode [mode | -show]
```

Availability

Admin

Description

Use these commands to enable media mode (GBIC or SFP) if the mode value is non-zero and disable the media mode if the mode value is 0. The mode is saved in flash memory and stays in that mode until the next execution of `setmediamode`, `setsfpmode`, or `setgbicmode`. The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

Media mode when enabled modifies the behavior of the diagnostic test methods so that ports without media installed are not tested. Normally tests such as `crossporttest` or `spinsilk` will fail if any port is not operating properly, but with media mode enabled the functional tests will be skipped on ports that do not contain media.

Operands

This command has the following operands:

mode	Specify 1 to enable media mode or 0 to disable media mode. If no mode is specified the current value is displayed. Any other value will enable media mode.
`-show`	Specify the `-show` operand to display the current setting. This operand is optional.

Example

To enable or disable media mode:

```
switch:admin> setgbicmode 1
GBIC mode is now 1 (Enabled).
switch:admin> setsfpmode 0
SFP mode is now 0 (disabled).
switch:admin> setmediamode -show
Media mode is now 0 (disabled).
```

See Also

```
crossporttest
itemlist
spinjitter
spinsilk
```

Example The following example shows how set error level of module named NS to value 3:

```
switch:admin> seterrlvl NS 3
```

See Also `dbgshow`

setesdmode

Enable or disable ESD mode.

Syntax `setesdmode [mode | -show]`

Availability Admin

Description Use this command to enable or disable ESD mode. The mode is saved in non-volatile memory and stays in that mode until the next execution of `setesdmode`.

The mode becomes active as soon as this command is executed. It does not require a reboot to take effect.

ESD mode when enabled modifies the behavior of the diagnostic test methods and post scripts. The exact behavior varies but most commonly consists of disabling the ports defined with `diagsetports` when `spinsilk` or other functional tests are run for ESD or EMI testing purposes.

Operands This command has the following operands:

mode	Specify 1 to enable ESD mode, specify 0 to disable ESD mode. This operand is optional.
`-show`	Specify this operand to display the current mode setting. This operand is optional.

If no operand is specified the current value is displayed.

Example **To set ESD mode:**

```
switch:admin> setesdmode
Esd Mode is 0 (Disabled).
switch:admin> setesdmode 1
Config update Succeeded
Esd Mode is now 1 (Enabled).
switch:admin>
```

See Also `spinsilk`

setdbg

Set debug level of the specified module.

Syntax `setdbg module_name level`

Availability Admin

Description Use this command to set the debug level of a specified module.

Operands This command has the following operands:

module_name	Specify the name of the module where you want to view the debug and verbosity levels. Module names are case sensitive. This operand is optional.
level	Specify the debug level for the specified module. This operand is required.

Example The following example shows how set debug level of module named NS to value 3:

```
switch:admin> setdbg NS 3
```

See Also dbgshow

seterrlvl

Set the error level of the specified module.

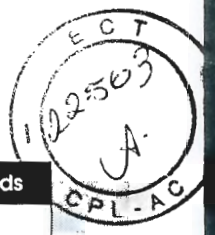
Syntax `seterrlvl module_name level`

Availability Admin

Description Use this command to set the error level of a specified module.

Operands This command has the following operands:

module_name	Specify the name of the module where the error level is to be set. Module names are case sensitive. This operand is required.
level	Specify the error level for the module. This operand is required.



- If you are logged into Logical switch 1, sensors 1 and 2 are for the two CPs in slots 5 and 6, respectively. Sensors 3 through 6 are for switch blade slots 7 through 10, respectively.
- If you are logged into the Active CP through the console port, you are prompted to specify the logical switch this command is executed on. If you login to the Active CP through the Fabric OS shell, this command always executes on the default switch (logical switch 0).
- Regardless of logical switch, sensors 7 through 9 are for the three chassis fans, left to right, and sensors 10 through 13 are for the four chassis power supplies, bottom to top.

Operands None

Example **To view the sensor values in a ED-12000B:**

```
switch:admin> sensorshow
sensor  1: (Temperature) is Ok, value is 39 C
sensor  2: (Temperature) is Absent
sensor  3: (Temperature) is Absent
sensor  4: (Temperature) is Absent
sensor  5: (Temperature) is Ok, value is 26 C
sensor  6: (Temperature) is Ok, value is 27 C
sensor  7: (Fan         ) is Ok, speed is 2537 RPM
sensor  8: (Fan         ) is Ok, speed is 2537 RPM
sensor  9: (Fan         ) is Ok, speed is 2556 RPM
sensor 10: (Power Supply ) is Ok
sensor 11: (Power Supply ) is Absent
sensor 12: (Power Supply ) is Ok
sensor 13: (Power Supply ) is Absent
switch:admin>
```

See Also

```
fanshow
tempshow
```

3. Reset the version stamp using the `secversionreset` command on each secure fabric to be merged into the controller fabric. The controller fabric does not require a version reset.
4. Cascade the fabrics together. When the secure fabrics are merged, the primary FCS switch in the controller fabric will propagate its security policies across the newly formed fabric.

When security mode is enabled, this command can only be issued from the primary FCS switch, a non-FCS when there is no FCS switch in the fabric, or on a disabled switch.

Operands None

Example **To reset the version stamp to zero:**

```
primaryfcs:admin> secversionreset
About to reset version stamp to 0.
Are you sure (yes, y, no, n):[no] y
Committing configuration... done.
Security Policy Version Stamp has been set to 0.
primaryfcs:admin>
```

See Also

```
secfabricshow
secmodeenable
secmodedisable
secmodeshow
sectransabort
```

sensorshow

Display sensor readings.

Syntax `sensorshow`

Availability All users

Description Use this command to display the current temperature, fan and power supply status and readings from sensors located on the switch. The actual location of the sensors varies depending on the switch type.

In the ED-12000B, the information returned with `sensorshow` is specific to the logical switch you are logged into:

- If you are logged into Logical switch 0, sensors 1 through 4 are for switch blade slots 1 through 4, respectively. Sensors 5 and 6 are for the two CPs in slots 5 and 6, respectively.

When security mode is enabled, this command can be executed from any switch in the fabric.

Operands None

Example **To abort the current security transaction:**

```
primaryfcs:admin> sectransabort
Transaction has been aborted.
primaryfcs:admin>
```

See Also

```
secpolicyabort
secpolicyactivate
secpolicyadd
secpolicycreate
secpolicydelete
secpolicyremove
secpolicysave
secpolicyshow
secpolicydump
```

secversionreset

Reset the version stamp to zero.

Syntax `secversionreset`

Availability Admin

Description Use this command to reset the version stamp of all switches in a fabric to zero, so that it can be joined to the another secure fabric.

When merging two or more secure fabrics, the following steps should be taken.

1. Determine which secure fabric will become the FCS_POLICY controller fabric, that is the dominant fabric to which all other secure fabrics will be merged.
2. Use the `secpolicyadd`, `secpolicyremove`, and `secpolicyactivate` commands to modify the FCS_POLICY of the merging fabrics to match the FCS_POLICY of the controller fabric. All secure fabrics to be merged must have identical FCS_POLICY lists. The FCS policies of merged fabrics must match exactly, that is, they must contain the same FCS members and in the same order, or the merge will fail.

command can enable the root or factory account on a non-FCS switch when you specify a password for those accounts.

The password should be at least 8 characters long and no more than 40 characters.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operand:

domain	Specify the Domain of a switch where you want to change the password. This operand is required.
login_name	Specify the login name where you want to change the password. This operand is required.

Example **To set the password on a remote switch with a Domain of 2:**

```
primaryfcs:admin> sectemppasswdset 2, "root"
Please provide password of root on primary FCS switch
in order to change this password: ********
Set remote switch root password: ********
Re-enter new password: ********
Account root has been successfully enabled on domain 2
```

See Also
- passwd
- secnonfcspasswd
- sectemppasswdreset
- secmodeenable
- secmodeshow
- secmodedisable

sectransabort

Abort current security transaction.

Syntax `sectransabort`

Availability Admin

Description Use this command to abort the current transaction. This command is used to recover from management application problems. This command will abort all current changes that have not been committed or activated.

Example To remove temporary passwords:

```
primaryfcs:admin> sectemppasswdreset 2, "root"
Account root has been successfully disabled on domain 2

primaryfcs:admin> sectemppasswdreset 2
Restoring password of every account on domain 2
Temporary password of each account on domain 2 has been successfully reset
   (if switch is non fcs switch it will further display).
Root and factory accounts on domain 2 have been disabled.

primaryfcs:admin> sectemppasswdreset
All temporary passwords or account settings have been restored to
fabric-wide secure settings.
Passwords of permanent accounts have been reset to fabric-wide
values. Root and factory accounts on each Non FCS switch have
been disabled.
```

See Also
- secswitchpasswd
- secnonfcspasswd
- secmodeenable
- secmodeshow

sectemppasswdset

Set a temporary password on a remote switch.

Syntax `sectemppasswdset` *domain, login_name*

Availability Admin

Description Use this command to set a unique temporary password for a given account on a specific switch in the fabric. Use the `sectemppasswdreset` command to remove the temporary password or reboot the switch.

You can change any password on any switch. In order to the change the password of an account which has higher level than that of the current user logged into the primary FCS switch, you must enter the password of the same level account on the primary FCS switch.

The password setup on the target is not persistent and will be reset to the secure fabric-wide setting when this target switch is rebooted or when `sectemppasswdreset` is run on primary FCS switch

Each switch has four accounts; Root, Factory, Admin and User. Root and Factory accounts are disabled for non-FCS switches. This

sectemppasswdreset

Reset a password on a remote switch.

Syntax `sectemppasswdreset [domain[, "login_name"]]`

Availability Admin

Description Use this command to remove temporary passwords that had been set up using `sectemppasswdset` command. The password is restored to the default password set up on non-FCS switches.

If a login name is not supplied, all passwords on the switch identified by the specified Domain are refreshed. If the Domain is also not supplied, all temporary passwords for all login levels are removed from every switch in the fabric.

Each switch has four accounts, Root, Factory, Admin and User. Root and Factory accounts are disabled for non-FCS switches. If they are temporarily activated by `sectemppasswdset`, those accounts are disabled by `sectemppasswdreset` or rebooting the switch.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

domain	Specify the Domain of the switch from which the temporary passwords are to be removed. This operand is optional.
login_name	Specify the name of the login account from which the temporary password are removed. This operand is optional.

This operand is optional and the default is all statistics. If the `list` operand is specified, then this operand is required.

list Specify a list of domains to display the security statistics on. Specify an asterisk (*) to represent all switches in the fabric or, specify a list of domains separated by semicolons. This operand is optional and the default value is the local switch.

Example **To display the MS_POLICY statistics on the local switch:**

```
primaryfcs:admin> secstatsshow "MS_POLICY"
Name      Value
====================
MS        20
primaryfcs:admin>
```

To display statistic information for the "TELNET_POLICY" for all switches in the fabric:

```
primaryfcs:admin> secstatsshow "TELNET_POLICY", "*"

Fabric Statistics:

Domain 1:
Name                Value
=========================================

TELNET_POLICY       0

Domain 69:
Name                Value
=========================================

TELNET_POLICY       0

Domain 70:
Name                Value
=========================================

TELNET_POLICY       0

primaryfcs:admin>
```

See Also `secfabricshow`
`secstatsreset`

Description Use this command to display security statistics for one or all security policies. This command can be issued to any switch. If issued on the Primary FCS switch, this command can retrieve and display the security statistics for any or all switches in the fabric.

When security mode is enabled, this command can be issued from any switch in the fabric.

Operands This command has the following operand:

name Specify the name of a security statistic you would like to view. If executed on the Primary FCS, specify an asterisk (*) to represent all security policies. Valid values for this operand are:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- DCC_POLICY
- LOGIN
- INVALID_TS
- INVALID_SIGN
- INVALID_CERT
- SLAP FAIL
- SLAP_BAD_PKT
- TS_OUT_SYNC
- NO_FCS
- INCOMP_DB
- ILLEGAL_CMD

The specified policy name must be all capitalized.

To access DCC policies, enter DCC_POLICY. Violations are not tracked for individual DCC policies. The statistics for all DCC_POLICY violations are grouped together.

- SLAP_BAD_PKT
- TS_OUT_SYNC
- NO_FCS
- INCOMP_DB
- ILLEGAL_CMD

The specified policy name must be all capitalized.

To access DCC policies, enter DCC_POLICY. Violations are not tracked for individual DCC policies. The statistics for all DCC_POLICY violations are grouped together.

This operand is optional and the default is all statistics. If the `list` operand is specified, then this operand is required.

list — Specify a list of domains to reset the security statistics on. Specify an asterisk (*) to represent all switches in the fabric or, specify a list of domains separated by semicolons. This operand is optional and the default value is the local switch.

Example **To reset all statistics on the local switch:**

```
primaryfcs:admin> secstatsreset
About to reset all security counters.
Are you sure (yes, y, no, n):[no] y
Security statistics reset to zero.
primaryfcs:admin>
```

To reset DCC_POLICY statistics on domains 1 and 69:

```
primaryfcs:admin> secstatsreset "DCC_POLICY", "1;69"
Reset DCC_POLICY statistic.
primaryfcs:admin>
```

See Also `secfabricshow`
`secstatsshow`

secstatsshow

Display security statistic for a policy or for all policies.

Syntax `secstatsshow [name][, list]`

Availability Admin

See Also

```
secpolicyabort
secpolicyactivate
secpolicyadd
secpolicycreate
secpolicydelete
secpolicyremove
secpolicysave
secpolicydump
```

secstatsreset

Reset security statistic for a policy or all policies to zero.

Syntax `secstatsreset [name][,list]`

Availability Admin

Description Use this command to reset statistic data for a particular policy or all policies to zero. This command can be issued to any switch. If issued on the Primary FCS switch, this command can reset security statistics for any or all switches in the fabric.

Operands This command has the following operand:

name Specify the name of a security statistic you would like to reset. If executed on the primary FCS, specify an asterisk (*) to represent all security policies. Valid values for this operand are:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- DCC_POLICY
- LOGIN
- INVALID_TS
- INVALID_SIGN
- INVALID_CERT
- SLAP FAIL

- SCC_POLICY
- OPTIONS_POLICY

The specified policy name must be capitalized.

The DCC_POLICY_nnn name has the common prefix DCC_POLICY_ followed by a string of user defined characters. These characters do not have to be capitalized like regular policy names, but is case sensitive.

This operand is optional.

Example **To display all security policies from all databases:**

```
primaryfcs:admin> secpolicyshow "active"
_____________________________________________________________

                ACTIVE POLICY SET

FCS_POLICY
   Pos    Primary WWN                        DId swName
   _____________________________________________________
     1    Yes     10:00:00:60:69:30:15:5c    1 primaryfcs

HTTP_POLICY
   IpAddr
   _____________________________________________________
   192.155.52.0

_____________________________________________________________
primaryfcs:admin>
primaryfcs:admin> secpolicyshow "defined"
_____________________________________________________________

                DEFINED POLICY SET

FCS_POLICY
   Pos    Primary WWN                        DId swName
   _____________________________________________________
     1    Yes     10:00:00:60:69:30:15:5c    1 primaryfcs

HTTP_POLICY
   IpAddr
   _____________________________________________________
   192.155.52.0
   192.155.53.1
   192.155.54.2
   192.155.55.3
   192.155.56.4

_____________________________________________________________
primaryfcs:admin>
```

secpolicyshow

Display an existing security policy.

Syntax `secpolicyshow [listtype[, name]]`

Availability Admin

Description Use this command to display the members of an existing policy in the Active, or Defined security policy database. Users can specify which database to display. If not specified, all database are displayed.

Users can specify to view a security policy by name. If no name is specified, all policies are displayed.

This command displays the policy database one page at a time. Use *secpolicydump* to display the policy database without page breaks.

When security mode is enabled, this command can be executed on any FCS switch in fabric.

Operands This command has the following operand:

listtype Specify which database to display. The name for active database is `Active`; the name for saved, defined database is `Defined`. This operand must be enclosed in quotation marks. If not specified, all databases are displayed. This operand is optional. Use an asterisk (*) to specify both Active and Defined.

name Specify the name of a security policy you would like to view. Valid values for this operand are:

- DCC_POLICY_nnn
- FCS_POLICY
- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY

```
secpolicyshow
secpolicydump
```

secpolicysave

Save a defined security policy to flash memory on all switches in the fabric.

Syntax `secpolicysave`

Availability Admin

Description Use this command to save a defined security policy to flash memory of all switches in the fabric.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands None

Example **To save new policy set in all switches in the fabric:**

```
primaryfcs:admin> secpolicysave
Committing configuration...done.
Saving Define FMPS ...
done
primaryfcs:admin>
```

See Also

```
secpolicyabort
secpolicyactivate
secpolicyadd
secpolicycreate
secpolicydelete
secpolicyremove
secpolicyshow
secpolicydump
```

The DCC_Policy_nnn is a list of devices associated with a specific switch and port combination. The device is specified with a WWN string. The switch and port combination must be specified in the following format:

`<switch><port>`

where:

`<switch>` can be specified using WWN, Domain, or switch name.

`<port>` can be specified by port number separated by commas, and enclosed in either brackets or parenthesis. For example, (2, 4, 6). Ports enclosed in brackets will include the devices currently attached to those ports. The following examples show several ways to specify the port values:

(1-6) = selects ports 1 through 6.

(*) = selects all ports on the switch.

[3, 9] = selects ports 3 and 9 and all devices attached to those ports.

[1-3, 5] = selects ports 1 through 3 and 5 and all devices attached to those ports.

[*] = selects all ports on the switch and devices currently attached to those ports.

OPTIONS_POLICY members

`"NoNodeWWNZoning"` is the only option.

Example **To remove a member that has a WWN of 12:24:45:10:0a:67:00:40 from MS policy:**

```
primaryfcs:admin> secpolicyremove "MS_POLICY", "12:24:45:10:0a:67:00:40"
Member(s) have been removed from MS_POLICY. .
primaryfcs:admin>
```

See Also

`secpolicyabort`
`secpolicyactivate`
`secpolicyadd`
`secpolicycreate`
`secpolicydelete`
`secpolicysave`

This operand is required.

member

Specify a member or list of members to delete from the policy. The members must be enclosed in quotation marks and separated by semicolons. This operand is required. Depending on the policy type, members can be specified using IP address, WWN, Domain, or switch name.

IP Address Member Policy Types

The following policy types require members be specified by IP address:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY

These policy types require member IDs in dot notation (for example, 124.23.56.122). If 0 is specified in one of the octets, it means any number can be matched.

WWN Member Policy Types

The following policy types require members be specified by WWN address:

- FCS_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY

These policy types require member IDs be specified as WWN strings, Domains, or switch names. If Domain or switch names are used, the switches associated must be present in the fabric or the command fails.

DCC_POLICY Members

secpolicyremove

Remove members from an existing policy.

Syntax `secpolicyremove "name", "member;member"`

Availability Admin

Description Use this command to remove members from an existing security policy. If a policy is empty after removing all members, all accesses to the policy are disallowed (the DCC_POLICY and OPTIONS_POLICY are an exception). You cannot remove all members from the FCS_POLICY, and you cannot remove the FCS members from the SCC_POLICY.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operands:

name Specify the name of an existing policy you want to remove members from. Valid values for this operand are:

- DCC_POLICY_nnn
- FCS_POLICY
- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- OPTIONS_POLICY

The specified policy name must be capitalized.

The DCC_POLICY policy name has the common prefix DCC_POLICY_ followed by a string of user defined characters. These characters do not have to be capitalized like regular policy names, but are case sensitive.

Example To move backup FCS switch at position 2 to position 3 in the FCS list:

```
switch5:admin> secpolicyfcsmove
Pos    Primary WWN                       DId swName.
================================================
  1    Yes     10:00:00:60:69:10:02:18    1 switch5.
  2    No      10:00:00:60:69:00:00:5a    2 switch60.
  3    No      10:00:00:60:69:00:00:13    3 switch73.

Please enter position you'd like to move from  : (1..3) [1] 2

Please enter position you'd like to move to  : (1..3) [1] 3

_____________________________________________________
                DEFINED POLICY SET

FCS_POLICY
 Pos    Primary WWN                       DId swName
 _____________________________________________________
  1    Yes     10:00:00:60:69:10:02:18    1 switch5.
  2    No      10:00:00:60:69:00:00:13    3 switch73.
  3    No      10:00:00:60:69:00:00:5a    2 switch60.

_____________________________________________________
switch5:admin>
```

See Also

- secfabricshow
- secpolicyabort
- secpolicyactivate
- secpolicyadd
- secpolicycreate
- secpolicydelete
- secpolicyremove
- secpolicysave
- secpolicyshow
- secpolicydump

secpolicyfcsmove

Move a member in the FCS policy.

Syntax `secpolicyfcsmove [From, To]`

Availability Admin

Description Use this command to move an FCS member from one position to another position in the FCS list. Only one FCS can be moved at a time. The first FCS switch in the list that is also present in the fabric is the primary FCS.

If no parameters are specified, the command becomes interactive and prompts for valid values for the operands.

This command must be issued from the primary FCS switch. If a backup FCS is moved to the first position, then it becomes the primary FCS after activation.

Operands This command has the following operands:

From	Specify the position number of the FCS switch you want to move.
To	Specify the position that you want to move the FCS switch to.

If no operand is specified the command becomes interactive and you are prompted for values.

To view all security policy information for the TELNET_POLICY without page breaks:

```
primaryfcs:admin> secpolicydump "*", "TELNET_POLICY"
_____________________________________________________
                DEFINED POLICY SET

  TELNET_POLICY
     IpAddr
     ___________________________________________________
     192.155.52.13
     192.155.52.11
  ___________________________________________________

  ___________________________________________________
                ACTIVE POLICY SET

  TELNET_POLICY
     IpAddr
     ___________________________________________________
     192.155.52.0

_____________________________________________________
  primaryfcs:admin>
```

See Also

secpolicyabort
secpolicyactivate
secpolicyadd
secpolicycreate
secpolicydelete
secpolicyremove
secpolicysave
secpolicyshow

The DCC_POLICY_nnn name has the common prefix DCC_POLICY_ followed by a string of user defined characters. These characters do not have to be capitalized like regular policy names.

This operand is optional.

Example **To view all security policy information from all databases (active, updating, defined) without page breaks:**

```
primaryfcs:admin> secpolicydump
_____________________________________________________
                DEFINED POLICY SET

  FCS_POLICY
     Pos    Primary WWN                      DId swName
     ____________________________________________________
       1    Yes     10:00:00:60:69:30:15:5c    1 primaryfcs

  HTTP_POLICY
     IpAddr
     ____________________________________________________
     192.155.52.0
  _____________________________________________________

  _____________________________________________________
                ACTIVE POLICY SET

  FCS_POLICY
     Pos    Primary WWN                      DId swName
     ____________________________________________________
       1    Yes     10:00:00:60:69:30:15:5c    1 primaryfcs

  HTTP_POLICY
     IpAddr
     ____________________________________________________
     192.155.52.0
     192.155.53.1
     192.155.54.2
     192.155.55.3

  _____________________________________________________
  primaryfcs:admin>
```

secpolicydump

Display all members of existing policies.

Syntax `secpolicydump [listtype[, name]]`

Availability Admin

Description Use this command to display the members of an existing policy in the Active and Defined (saved) databases with no page breaks.

When security mode is enabled, this command can be executed on any FCS switch in fabric.

Operands This command has the following operand:

listtype Specify which database to display. The name for active database is `Active`; the name for saved, defined database is `Defined`. If not specified, all databases are displayed. This operand is optional. An asterisk (*) can be used to specify both Active and Defined.

name Specify the name of a security policy you would like to view. Valid values for this operand are:

- DCC_POLICY_nnn
- FCS_POLICY
- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- OPTIONS_POLICY

The specified policy name must be capitalized.

- FRONTPANEL_POLICY
- SCC_POLICY
- OPTIONS_POLICY

The specified policy name must be capitalized.

The DCC_POLICY_nnn name has the common prefix DCC_POLICY_ followed by a string of user defined characters. These characters do not have to be capitalized like regular policy names.

This operand is required.

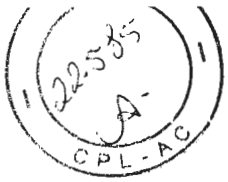
Once a Security policy is deleted, fabric wide switch access through that method is unrestricted.

Example **To delete an existing security policy:**

```
primaryfcs:admin> secpolicydelete "MS_POLICY"
About to delete policy MS_POLICY.
Are you sure (yes, y, no, n):[no] y
MS_POLICY has been deleted.
primaryfcs:admin>
```

See Also

```
secpolicyabort
secpolicyactivate
secpolicyadd
secpolicycreate
secpolicyremove
secpolicysave
secpolicyshow
secpolicydump
```




```
secpolicyremove
secpolicysave
secpolicyshow
secpolicydump
```

secpolicydelete

Delete an existing policy.

Syntax `secpolicydelete "name"`

Availability Admin

Description Use this command to delete an existing defined policy. The FCS_POLICY can not be deleted through this command, since this policy must exist to maintain security mode.

Each policy corresponds to a management method. The list of members of a policy acts as an access control list for that management method. When security mode is first enabled using the `secmodeenable` command only the FCS_POLICY exists. Before a policy is created, there is no enforcement for that management method, that is, all access is granted. After a policy has been created and a member has been added to the policy, that policy becomes closed to all access except from included members. If the policy is deleted all access is granted.

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands This command has the following operand:

name Specify the name of a security policy to delete. The policy name must be enclosed in quotation marks. Valid security policy names are:

- DCC_POLICY_nnn
- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY

This policy type requires member IDs be specified as WWN strings, Domains, or switch names. If Domain or switch names are used, the switches associated must be present in the fabric or the command fails.

To add all switches in the current fabric as members of the SCC_POLICY enter an asterisk "*" enclosed in quotation marks as the member value. This feature cannot be used by the other security telnet commands.

Example **To create a new single MS_POLICY that enables access through a device that has WWN of 12:24:45:10:0a:67:00:40:**

```
primaryfcs:admin> secpolicycreate "MS_POLICY", "12:24:45:10:0a:67:00:40"
MS_POLICY has been created.
primaryfcs:admin>
```

To create a new Front Panel policy that only enables Domains 3 and 4 to use the front panel:

```
primaryfcs:admin> secpolicycreate "FRONTPANEL_POLICY", "3; 4"
FRONTPANEL_POLICY has been created.
primaryfcs:admin>
```

To create a Device policy to allow 2 devices to attach to Domain 3 ports 1 and 3. The WWN of first device is 11:22:33:44:55:66:77:aa, and the WWN of second device is 11:22:33:44:55:66:77:bb:

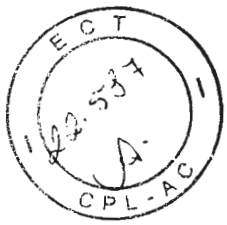
```
primaryfcs:admin> secpolicycreate "DCC_POLICY_aB_7",
   "11:22:33:44:55:66:77:aa;11:22:33:44:55:66:77:bb;3[1,3]"
DCC_POLICY_abc has been created.
primaryfcs:admin>
```

To create a Telnet policy to allow anyone on the 192.168.5.0/24 network to access the fabric through sectelnet:

```
primaryfcs:admin> secpolicycreate "TELNET_POLICY", "192.168.5.0"
TELNET_POLICY has been created.
primaryfcs:admin>
```

See Also

```
secpolicyabort
secpolicyactivate
secpolicyadd
secpolicydelete
```



- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY

These policy types require member IDs be specified as WWN strings, Domains, or switch names. If Domain or switch names are used, the switches associated must be present in the fabric or the command fails.

DCC_POLICY Members

The DCC_Policy_nnn is a list of devices associated with a specific switch and port combination. The device is specified with a WWN string. The switch and port combination must be in the following format:

`<switch><port>`

where:

`<switch>` can be specified using WWN, Domain, or switch name.

`<port>` can be specified by port number separated by commas, and enclosed in either brackets or parenthesis. For example, (2, 4, 6). Ports enclosed in brackets will include the devices currently attached to those ports. The following examples show several ways to specify the port values:

(1-6) = selects ports 1 through 6.

(*) = selects all ports on the switch.

[3, 9] = selects ports 3 and 9 and all devices attached to those ports.

[1-3, 5] = selects ports 1 through 3 and 5 and all devices attached to those ports.

[*] = selects all ports on the switch and devices currently attached to those ports.

OPTIONS_POLICY members

`"NoNodeWWNZoning"` is the only option.

SCC_POLICY Members

- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- OPTIONS_POLICY

The specified policy name must be capitalized.

The DCC_POLICY_nnn name has the common prefix DCC_POLICY_ followed by a string of user defined characters. These characters do not have to be capitalized like regular policy names. Valid values for DCC_POLICY_nnn are user defined alphanumeric or underscore characters. The maximum length is 30 characters, including the prefix DCC_POLICY_.

member Specify a list of members for the security policy. The members must be enclosed in quotation marks and separated by semicolons. Depending on the Policy type members can be specified using IP address, WWN, Domain, or switch name.

IP Address Member Policy Types

The following policy types require members be specified by IP address:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY

These policy types require member IDs in dot notation (for example, 124.23.56.122). If 0 is specified in one of the octets, it means any number can be matched.

WWN Member Policy Types

The following policy types require members be specified by WWN address:

secpolicycreate

Create a new policy.

Syntax `secpolicycreate name[, "member;member"]`

Availability Admin

Description Use this command to create a new policy. All policies can be created only once, except for the DCC_POLICY_nnn. Each DCC_POLICY_nnn must each have a unique name.

Adding members while creating a policy is optional. You may add members to a policy later, using the `secpolicyadd` command.

Each policy corresponds to a management method. The list of members of a policy acts as an access control list for that management method. When security mode is first enabled using the `secmodeenable` command only the FCS_POLICY exists. Before a policy is created, there is no enforcement for that management method, that is, all access is granted. After a policy has been created and a member has been added to the policy, that policy becomes closed to all access except from included members. If all members are then deleted from the policy, all access is denied for that management access method.

The FCS_POLICY can only be created when enabling security mode using the `secmodeenable` command.

If a TELNET_POLICY or SERIAL_POLICY is created that will end the current sectelnet or serial session, a warning is issued.

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Operands This command has the following operand:

name Specify the name of a policy you want to create. Valid values for this operand are:

- DCC_POLICY_nnn
- FCS_POLICY
- TELNET_POLICY

(*) = selects all ports on the switch.

[3, 9] = selects ports 3 and 9 and all devices attached to those ports.

[1-3, 5] = selects ports 1 through 3 and 5 and all devices attached to those ports.

[*] = selects all ports on the switch and devices currently attached to those ports.

OPTIONS_POLICY members

"NoNodeWWNZoning" is the only option.

Example **Adding a member to the MS_POLICY using the device WWN:**

```
primaryfcs:admin> secpolicyadd "MS_POLICY", "12:24:45:10:0a:67:00:40"
Member(s) have been added to MS_POLICY.
primaryfcs:admin>
```

Adding an SNMP manager to WSNMP_POLICY:

```
primaryfcs:admin> secpolicyadd "WSNMP_POLICY", "192.168.5.21"
Member(s) have been added to WSNMP_POLICY.
primaryfcs:admin>
```

See Also

- secpolicyabort
- secpolicyactivate
- secpolicycreate
- secpolicydelete
- secpolicyremove
- secpolicysave
- secpolicyshow
- secpolicydump

- RSNMP_POLICY
- WSNMP_POLICY

These policy types require member IPs to be specified in dot notation (for example, 124.23.56.122). If 0 is specified in one of the octets, it means any number can be matched.

WWN Member Policy Types

The following policy types require members be specified by WWN address:

- FCS_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY

These policy types require members be specified as WWN strings, Domain ID, or switch names. If Domain ID or switch names are used, the switches associated must be present in the fabric or the command fails.

DCC_POLICY Members

The DCC_POLICY_nnn is a list of devices associated with a specific switch and port combination. An empty DCC_POLICY does not stop access to the switch. The device is specified with a WWN string. The switch and port combination must be in the following format:

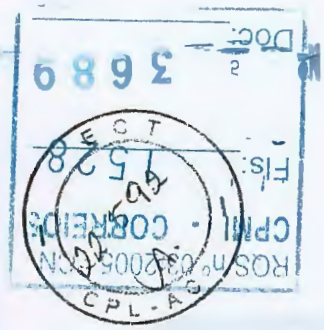
```
<switch><port>
```

where:

`<switch>` can be specified using WWN, Domain, or switch name.

`<port>` can be specified by port number separated by commas, and enclosed in either brackets or parenthesis. For example, (2, 4, 6). Ports enclosed in brackets will include the devices currently attached to those ports. The following examples show several ways to specify the port values:

(1-6) = selects ports 1 through 6.



the policy, all access is denied for that management access method (the DCC_POLICY and OPTIONS_POLICY are an exception).

When security mode is enabled, this command can only be issued from the primary FCS switch.

Operands

This command has the following operands:

name

Specify the name of an existing policy you want to add members to. Valid values for this operand are:

- DCC_POLICY_nnn
- FCS_POLICY
- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- OPTIONS_POLICY

The specified policy name must be capitalized.

The DCC_POLICY_nnn name has the common prefix DCC_POLICY_ followed by a string of user defined characters. These characters do not have to be capitalized like regular policy names, but are case sensitive.

member

Specify a list of member switches for the security policy. The members must be enclosed in quotation marks and separated by semicolons. Depending on the Policy type members can be specified using IP address, WWN, Domain, switch name, or other.

IP Address Member Policy Types

The following policy types require members be specified by IP address:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example **To activate the defined security policy set to all switches in the fabric:**

```
primaryfcs:admin> secpolicyactivate
About to overwrite the current Active data.
ARE YOU SURE (yes, y, no, n): [no] y
Committing configuration...done.
Saving Defined FMPS ...
done
Saving Active FMPS ...
done
primaryfcs:admin>
```

See Also

```
secpolicyabort
secpolicyadd
secpolicycreate
secpolicydelete
secpolicyremove
secpolicysave
secpolicyshow
secpolicydump
```

secpolicyadd

Add members to an existing policy.

Syntax `secpolicyadd "name", "member; member"`

Availability Admin

Description Use this command to create a new policy. All policies can be created only once, except for the DCC_POLICY_nnn. Each DCC_POLICY_nnn must each have a unique name.

Each policy corresponds to a management method. The list of members of a policy acts as an access control list for that management method. When security is first enabled using the `secmodeenable` command only the FCS_POLICY exists. Before a policy is created, there is no enforcement for that management method, that is, all access is granted. After a policy has been created and a member has been added to the policy, that policy becomes closed to all access except from included members. If all members are then deleted from

secpolicyabort

Aborts all changes to the defined database that have not been saved.

Syntax `secpolicyabort`

Availability Admin

Description Use this command to abort all changes to the defined security database that have not been saved to flash memory.

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example **To abort all changes that have not been saved to flash memory:**

```
primaryfcs:admin> secpolicyabort
Unsaved data has been aborted.
primaryfcs:admin> secpolicyabort
No new data to abort.
```

See Also

```
secpolicyactivate
secpolicyadd
secpolicycreate
secpolicydelete
secpolicyremove
secpolicysave
secpolicyshow
secpolicydump
```

secpolicyactivate

Apply defined policy set to all switches in the fabric.

Syntax `secpolicyactivate`

Availability Admin

Description Use this command to activate the current defined security policy to all switches in the fabric. After activation the defined policy set becomes the active policy set.

secnonfcspasswd

Set the admin password for non-FCS switches.

Syntax `secnonfcspasswd`

Availability Admin

Description Use this command to change the admin password on all non-FCS switches in the fabric. This command can only be issued from the Primary FCS switch in secure mode. The changed passwords are persistent across reboots. All non-FCS switches that join the fabric in the future will inherit this new password.

This command also disables the root and factory accounts on all non-FCS switches in the fabric.

The password must be between 8 and 40 characters long, and may consist of any combination of alpha-numeric characters.

Make sure no users are logged into the network when this command is executed. All users logged into the fabric as admin on non-FCS switches will have their sessions terminated.

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example **To set the admin password for all non-FCS switches in the fabric:**

```
primaryfcs:admin> secnonfcspasswd
Non FCS switch password:
Re-enter new password:
Committing configuration...done.
primaryfcs:admin>
```

See Also

```
passwd
sectemppasswdset
secmodeenable
secmodeshow
secmodedisable
```

secmodeshow

Display if security mode is enabled or disabled.

Syntax `secmodeshow`

Availability Admin

Description Use this command to display the current security mode of the fabric. The fabric can be in secure mode or non secure mode. If the fabric is in secure mode, the following information is displayed:

- Version stamp - Displays the current version and build date and time of the security database.
- FCS switches - Displays a list of FCS switches.
- Primary - Displays whether the switch is a Primary FCS or Backup FCS.
- WWN - Displays the WWN of the FCS switch.
- Did - Displays the Domain of the FCS switch.
- swName - Displays the alias name of the FCS switch.

When security mode is enabled, this command can be executed on any switch in fabric.

Operands None

Example **To display the current security mode of a fabric:**

```
primaryfcs:admin> secmodeshow
   Secure Mode: ENABLED.
   Version Stamp: 9182, Wed Mar 13 16:37:01 2001.
   POS  Primary  WWN                       DId    swName
   ==========================================
   1    Yes      10:00:00:60:69:00:00:5a   21     SW47
   2    No       12:00:00:60:60:03:23:5b    5     SW12
   primaryfcs:admin>
```

See Also `secfabricshow`
`secmodeenable`
`secmodedisable`

Example To enable a security policy that includes three FCS switches specified by Domain, WWN address, and switch name:

```
fcsprimary:admin> secmodeenable

Your use of the certificate-based security features of the software
   installed on this equipment is subject to the End User License Agreement
   provided with the equipment and the Certification Practices Statement,
   which you may review at http://www.switchkeyactivation.com/cps. By using
   these security features, you are consenting to be bound by the terms of
   these documents. If you do not agree to the terms of these documents,
   promptly contact the entity from which you obtained this software and do
   not use these security features.
   Do you agree to these terms? (yes, y, no, n): [no] y

   This is an interactive session to create a FCS list.

   Current FCS list is empty
   Enter WWN, Domain, or switch name(Leave blank when done): 2
   Switch WWN is 10:00:00:60:69:11:fc:53

   Current FCS list:
     10:00:00:60:69:11:fc:53

   Enter WWN, Domain, or switch name(Leave blank when done): 1
   Switch WWN is 10:00:00:60:69:11:fc:55

   Current FCS list:
     10:00:00:60:69:11:fc:53
     10:00:00:60:69:11:fc:55

   Enter WWN, Domain, or switch name(Leave blank when done):
   Are you done?  (yes, y, no, n): [no] y
   Is the FCS correct?  (yes, y, no, n): [no] y
   New FCS switch root password:
   Password must differ by at least 1 position
   New FCS switch root password:
   Re-enter new password:
   New FCS switch factory password:
   Re-enter new password:
   New FCS switch admin password:
   Re-enter new password:
   New FCS switch user password:
   Re-enter new password:
   New Non FCS switch admin password:
   Re-enter new password:
   Saving passwd...done.
   Saving Defined FMPS ...
   done
   Saving Active FMPS ...
   done
   Committing configuration...done.
   Secure mode is enabled.
   Saving passwd...done.
   Rebooting...
```

See Also secfabricshow
secmodedisable

If the fabric is not in secure mode and this command is issued, the switch reboots.

If the fabric is in secure mode and no FCS switches are present in the fabric, the command can be issued on any switch. This is used to recover a secure fabric that has no FCS switch.

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Make sure that all users (using Fabric OS CLI or Web Tools) are logged off the fabric before enabling security mode. All users who are logged into the fabric on non-FCS switches when this command executes have their telnet sessions terminated.

Operands This command has the following operand:

`fcsmember` Specify a list of FCS switches. The list of member switches must be enclosed in quotation marks and each member switch must be separated by semicolons. The members can be specified using Domain, WWN, or switch name format. For example:

```
"5; 10:00:00:60:69:00:00:20; star1"
```

If a member is specified by Domain, or switch name, the switch must be in the fabric or the command fails. This operand is optional. If no operand is specified the session becomes interactive and you are prompted to enter FCS member values.

secmodeenable

Enable security mode.

Syntax `secmodeenable ["fcsmember;fcsmember"]`

Availability Admin

Description Use this command to enable security mode on all switches in the fabric. This command fails if any switch in the fabric is not capable of enforcing the security policies defined in the security database. If no operand is specified the command becomes interactive.

`sectelnet` must be used to open a secure telnet session into a switch.

This command sets up security in the fabric by executing the following:

- activates security mode on all switches in the fabric
- creates the security database populated with a list of FCS switches in the FCS_POLICY
- distributes the security database to all switches in the fabric
- resets the root, factory, admin, and user account passwords on all FCS switches
- resets the admin account password on all Non FCS switches
- disables the root, factory, and user accounts on all non-FCS switches in the fabric

The administrator is prompted to enter passwords for the following accounts:

- factory
- root
- admin
- user

If the fabric is not in secure mode and one or more specified FCS switches are present in the fabric, the command must be issued on the first active FCS in the list.

If the fabric is not in secure mode and no specified FCS switches are present in the fabric, the command can be issued on any switch.

secmodedisable

Disable security mode.

Syntax `secmodedisable`

Availability Admin

Description Use this command to disable security mode on all switches in the fabric. This command deletes both the defined and active security database.

When security mode is enabled, this command can only be issued from the Primary FCS switch.

Operands None

Example **To disable security mode:**

```
primaryfcs:admin> secmodedisable
Warning!!!
About to disable security.
ARE YOU SURE (yes, y, no, n): [no] y
Committing configuration...done.
Removing Active FMPS...
done
Removing Defined FMPS...
done
Disconnecting current session.
```

See Also
`secfabricshow`
`secmodeenable`
`secmodeshow`

sechelp

Display information about security telnet commands.

Syntax `sechelp`

Availability Admin

Description Use this command to display a list of security telnet commands.

Operands None

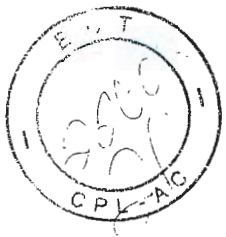
Example **To display a list of security telnet commands:**

```
switch:admin> sechelp

secFabricShow              Display security related fabric information
secFCSFailover             Force primary role to this FCS switch
secModeEnable              Enable security mode
secModeDisable             Disable security mode
secModeShow                Show current mode of security
secNonFCSPasswd            Set non FCS password
secPolicyAbort             Abort changes to defined policy
secPolicyActivate          Activate all policy sets
secPolicyAdd               Add members to a policy
secPolicyCreate            Create a policy
secPolicyDelete            Delete a policy
secPolicyFCSMove           Move a FCS member in the FCS list
secPolicyRemove            Remove members from a policy
secPolicySave              Save all policy sets and send to switches
secPolicyShow              Show members of one or more policies
secPolicyDump              Dump all policies
secStatsReset              Reset security statistics
secStatsShow               Display security statistics
secTempPasswdSet           Set temporary password
secTempPasswdReset         Reset temporary password
secTransAbort              Abort current transaction
secVersionReset            Reset version stamp

switch:admin>
```

Example To view the current security state:

```
primaryfcs:admin> secglobalshow
----General Security Infor----
flag 1, saveflag 1
transId 0
Queue Size 0
final Rca 0
reliablemsg 0
reliablePhase 0
Primary pub key: Exist
Primary Version 2
Primary WWN 10:00:00:60:69:90:02:53
Stamp 763828637
----The latest RCS STATUS----
RCS was enabled
sec_aca: free
RCS latest Phase: Completion
RCS Message ==> RCS transaction completes.
----DataBase STATUS----
Retry 0
Security Active DataSize 59 bytes
Active Sum 9c2a
Security Defined DataSize 59 bytes
Define Sum 9c2a
Zone Size 432 bytes
Zone sum 1855
sec_db: free
primaryDLPhase 6
----wwnDL State-----
domain 107 state 6
pid     tid     key     sec     usec
       769             6151       87052037      1048204774          173586
       769             6151       87052037      1048204774          173648
       769             6151       87052037      1048204775          441107
primaryfcs:admin>
```

See Also `secactivesize`
`secdefinesize`



Example To enable a Backup FCS switch to take over as the Primary FCS switch:

```
switch:admin> secfcsfailover
This switch is about to become the Primary FCS switch.
   All transactions of the current Primary FCS switch will be aborted.
   ARE YOU SURE  (yes, y, no, n): [no] y

   WARNING!!!
   The FCS policy of Active and Defined Policy sets have been changed.
   Review them before you issue secPolicyActivate again.
   switch:admin>
```

See Also
```
secfabricshow
secmodeenable
secmodedisable
secmodeshow
```

secglobalshow

Display the current internal security state information.

Syntax `secglobalshow`

Availability Admin

Description Use this command to display security server (secd) specific information as a snapshot of its current state. The information may include some of the following:

- The version and general information.
- The current status of the RCS transaction.
- The active and defined sizes of the security database.

This command is strictly intended for debugging purposes by technical support staff only. The information displayed may not be supported between releases and is subject to change arbitrarily.

When security mode is enabled, this command can be executed on any switch in fabric.

Operands None

Example To display security related fabric information on the Primary FCS switch:

```
switch:admin> secfabricshow
Role    WWN                     DId Status  Enet IP Addr    Name
   ==========================================================
   non-FCS 10:00:00:60:69:10:03:23   1 Ready   192.168.100.148 "nonfcs"
   Backup  10:00:00:60:69:00:12:53   2 Ready   192.168.100.147 "backup"
   Primary 10:00:00:60:69:22:32:83   3 Ready   192.168.100.135 "switch"
   ----------------------------------------------------------

Secured switches in the fabric: 3
switch:admin>
```

See Also `secpolicyshow`
`secpolicydump`

secfcsfailover

Enables a Backup FCS switch to take over as Primary FCS switch.

Syntax `secfcsfailover`

Availability Admin

Description Use this command to enable a Backup FCS switch to take over as the Primary FCS switch.

This command can only be issued on a Backup FCS switch. After this command is issued, the current Primary FCS switch will abort its current transaction and move the Backup FCS switch where this command is issued to be the first member in the FCS list. The current Primary FCS switch will then activate the new policy set and the Backup FCS switch which issued this command will become the new Primary FCS switch in the fabric.

The purpose of this command is to recover from a scenario where all available access to the Primary FCS switch is lost, such as the Ethernet and serial connections.

Operands None

secfabricshow

Displays security related fabric information.

Syntax `secfabricshow`

Availability Admin

Description This command displays the security related information about the fabric.

The information displayed is as follows:

Role	Displays whether the switch is the Primary FCS, Backup FCS, or Non FCS.
WWN	Displays the world wide name of the switch.
DId	Displays the Domain of the switch.
Status	Displays the security state of the switch. Ready - This switch is in a stable state. Busy - This switch is updating its security database. Error - This switch's security database is inconsistent with the Primary FCS.
Enet IP Addr	Displays the Ethernet IP address.
Name	Displays the switch name.

When security mode is enabled, this command can be executed on any switch in fabric.

Operands None

secdefinesize

Display the size of the defined security database.

Syntax `secdefinesize`

Availability Admin

Description Use this command to display the size of the active security database as *transaction* and *committed*. The *transaction* is the memory allocated by the security daemon to store the data. It's very close to the size sent to other switches and the size of Defined Security policies. The *committed* is how much space on disk it takes to store this information.

The *commit size* has a maximum of 64K. The *transaction size* has a maximum of 62K. If the commit size value is greater than 16 KB, then a 2.6 switch will not accept the data.

This command is strictly intended for debugging purposes by technical support staff only. The information displayed may not be supported between releases and is subject to change arbitrarily.

When security mode is enabled, this command can be issued from any switch in the fabric.

Operands None

Example **To display the size of the defined security database:**

```
primaryfcs:admin> secdefinesize
Size of Defined Security Database:
  committed: 1088 bytes (max 65536)
  transaction: 59 bytes
```

See Also
`secglobalshow`
`secactivesize`

secactivesize

Display the size of the active security database.

Syntax `secactivesize`

Availability Admin

Description Use this command to display the size of the active security database as *transaction* and *committed*. The *transaction* is the memory allocated by the security daemon to store the data. It's very close to the size sent to other switches and the size of Defined Security policies. The *committed* is how much space on disk it takes to store this information.

The *commit size* has a maximum of 64K. The *transaction size* has a maximum of 62K. If the commit size value is greater than 16 KB, then a 2.6 switch will not accept the data.

This command is strictly intended for debugging purposes by technical support staff only. The information displayed may not be supported between releases and is subject to change arbitrarily.

When security mode is enabled, this command can be issued from any switch in the fabric.

Operands None

Example **To display the size of the active security database:**

```
primaryfcs:admin> secactivesize
Size of Active Security Database:
  committed: 1088 bytes (max 65536)
  transaction: 59 bytes
```

See Also

```
secglobalshow
secdefinesize
```

```
switch:admin> savecore
following 2 directories contains core files:
          [ ]0: /core_files/nsd
          [ ]1: /core_files/zoned

Welcome to core files management utility.

          Menu
          1(or R): Remove all core files
          2(or F): FTP all core files
          3(or r): Remove marked files
          4(or f): FTP marked files
          5(or m): Mark Files for action
          6(or u): Un Mark Files for action
          9(or e): Exit

Your choice: m
Enter File Number to mark: 1
Enter CR To Continue....

following 2 directories contains core files:
          [ ]0: /core_files/nsd
          [*]1: /core_files/zoned

Welcome to core files management utility.


          Menu
          1(or R): Remove all core files
          2(or F): FTP all core files
          3(or r): Remove marked files
          4(or f): FTP marked files
          5(or m): Mark Files for action
          6(or u): Un Mark Files for action
          9(or e): Exit

Your choice: r
          /core_files/zoned

                  You have opted to remove core files under these directories:-
Please confirm (Y/[N]): y
Removing files....
removing core files under: /core_files/zoned
Done!
switch:admin>
```

To FTP core files using the savecore management utility:

```
switch:admin> savecore
following 1 directories contains core files:
        [ ]0: /core_files/zoned

        Welcome to core files management utility.

        Menu
        1(or R): Remove all core files
        2(or F): FTP all core files
        3(or r): Remove marked files
        4(or f): FTP marked files
        5(or m): Mark Files for action
        6(or u): Un Mark Files for action
        9(or e): Exit

Your choice: F
/core_files/zoned
You have opted to FTP these core files:-
Please confirm (Y/[N]): y
Destination IP Address? 192.168.10.10
User Name [anonymous]? jsmith
Remote Directory [.]? brcd
Password: **********
/core_files/zoned/core.8323:                    1.12 kB  382.40 B/s
Files transferred successfully!
switch:admin>
```

To remove core files from a selected directory:

To FTP selected core file directories:

```
switch:admin> savecore -h 192.168.204.188 -u jsmith -d core_files_here -p
   password
-f /core_files/zoned/,/mnt/core_files/nsd/
/core_files/zoned//core.1234:                    1.12 kB  382.60 B/s
/core_files/zoned//core.5678:                    1.12 kB  381.95 B/s
/mnt/core_files/nsd//core.873:                   1.12 kB  382.53 B/s
Files transferred successfully!
switch:admin>
```

To remove all core files using the savecore management utility:

```
switch:admin> savecore
following 1 directories contains core files:
        [ ]0: /mnt/core_files/panic

        Welcome to core files management utility.

        Menu
        1(or R): Remove all core files
        2(or F): FTP all core files
        3(or r): Remove marked files
        4(or f): FTP marked files
        5(or m): Mark Files for action
        6(or u): Un Mark Files for action
        9(or e): Exit

Your choice: 1
        /mnt/core_files/panic

        You have opted to remove ALL core files:-
Please confirm (Y/[N]): y
Removing files....
 removing core files under: /mnt/core_files/panic
Done!
switch:admin>
switch:admin> savecore
No core files found!
switch:admin>
```


```
switch:admin>
```

To remove selected core files from a CP:

```
switch:admin> savecore -r
   /core_files/panic/,/core_files/zoned/,/mnt/core_files/
   nsd/
Removing: /core_files/panic/
Removing: /core_files/zoned/
Removing: /mnt/core_files/nsd/
switch:admin>
```

To remove selected core files from the CP (using multiple -r operands):

```
switch:admin> savecore -r /core_files/panic/ -r
   /core_files/zoned/,/mnt/core_files
/nsd/
Removing: /core_files/panic/
Removing: /core_files/zoned/
Removing: /mnt/core_files/nsd/
switch:admin>
```

To remove all core files:

```
switch:admin> savecore -R
removing core files under: /core_files/panic
removing core files under: /core_files/zoned
removing core files under: /mnt/core_files/nsd
removing core files under: /mnt/core_files/panic
switch:admin>
```

To FTP all core files:

```
switch:admin>  savecore -h 192.168.204.188 -u jsmith -d core_files_here -p
   fexosophy  -F
/core_files/panic/core.873:                    1.12 kB   381.87 B/s
/core_files/zoned/core.1234:                   1.12 kB   382.14 B/s
/core_files/zoned/core.5678:                   1.12 kB   382.50 B/s
/mnt/core_files/nsd/core.873:                  1.12 kB   381.93 B/s
/mnt/core_files/panic/core.873:                1.12 kB   381.90 B/s
Files transferred successfully!
switch:admin>
```

Description Use this command to FTP core files, to remove core files, or to list core files. With no arguments, savecore will enter into interactive mode.

Options This command has the following options:

`-h ip-address` Specify a host-name if FTP requires it.

`-u user_name` Specify a user-name for login in the above host-name default will be anonymous.

`-p password` Specify a password for the above user-name.

`-a` Specify to use anonymous FTP to download the core files. This option cannot be used with **-u** option.

`-d remote_directory`
Specify the name of the remote directory into which the core files are copied into. The directory will be created if it does not already exists. It is assumed that the user has sufficient privilege to create files at this location.

`-f core-file-directory-list`
Specify a list of the core file directories to transfer to a remote site. This list can be comma (,) separated directory list or just a single directory name. Only the standard core files directories can be specified (`/core_files` and `/mnt/core_files`); all other files or directories are ignored.

`-R` Specify this option to remove all core files.

`-r <core-files-directory-list>`
Specify this option to remove core files under the directory list given. Removes all the core files under the listed directories. The directory list is a comma separated list of core files directory and other files, if any, will be ignored. No confirmation will be made before removal.

`-l` Specify this option to list all core files.

Example **To list all core files in a CP:**

```
switch:admin> savecore -l
/core_files/panic/core.873
/core_files/zoned/core.1234
/core_files/zoned/core.5678
/mnt/core_files/nsd/core.873
/mnt/core_files/panic/core.873
```

Example To view a list of routing related commands:

```
switch:admin> routehelp

bcastShow               Print broadcast tree information
dlsReset                Turn off Dynamic Load Sharing
dlsSet                  Turn on Dynamic Load Sharing
dlsShow                 Print state of Dynamic Load Sharing
fspfShow                Print FSPF global information
interfaceShow           Print FSPF interface information
iodReset                Turn off In-Order Delivery
iodSet                  Turn on In-Order Delivery
iodShow                 Print state of In-Order Delivery
linkCost                Set or print the FSPF cost of a link
LSDbShow                Print Link State Database entry
mcastShow               Print multicast tree information
nbrStateShow            Print neighbor's summary information
nbrStatsClear           Reset FSPF neighbor's counters
topologyShow            Print paths to domain(s)
uRouteConfig            Configure static unicast route
uRouteRemove            Remove static unicast route
uRouteShow              Print port's unicast routing info

switch:admin>
```

See Also `bcastshow`
`interfaceshow`
`urouteshow`

savecore

Save or remove core files created by daemons.

Syntax To FTP core files:

`savecore [[-f <core-file-list>]... | -F] [-h ip-address] [-u user_name | -a] [-p password] [-d remote_directory]`

To Remove core files:

`savecore [[-r <core-files-directory-list>]... | -R ]`

To list core files:

`savecore -l`

Availability Admin

Example To reboot the switch:

```
switch:admin> reboot
Warning: This command is being run on a control processor (CP)
based system and will cause the active CP to reboot. This will
cause disruption to devices attached to both switch 0 and switch 1.
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
```

See Also
```
fastboot
switchreboot
```

routehelp

Display routing help commands.

Syntax `routehelp`

Availability All users

Description Use this command to display routing help commands.

Operands None

mode Specify 1 to display the contents of RAM, specify 0 to display the contents of the transaction buffer. The default value is 0. This operand is optional.

Example **To display all QuickLoops beginning with the letter "q":**

```
switch:admin> qloopshow "q*"
qloop: qlp110:00:00:60:69:00:60:11
10:00:00:60:69:00:30:02
 qloop: qlp210:00:00:60:69:00:60:13
```

See Also

```
qloopadd
qloopcreate
qloopdelete
qloopremove
```

reboot

Reboot the switch.

Syntax `reboot`

Availability Admin

Description Use this command to reboot the switch. The reboot takes effect immediately as the switch resets, then executes the normal power-on booting sequence.

While the switch is rebooting, the command line session is closed and all fibre channel ports are inactive. If the switch was part of a fabric, the remaining switches reconfigure.

For the ED-12000B, the `reboot` command will reboot both logical switches and both CPs. A confirmation message is displayed to verify that you want to `reboot` the switch.

Operands None

See Also

`qloopadd`
`qloopcreate`
`qloopdelete`
`qloopshow`

qloopshow

Display QuickLoop information.

Syntax `qloopshow [pattern] [, mode]`

Availability All users

This command requires a Zoning license.

Description Use this command to display QuickLoop configuration information.

If no parameters are specified, all zone configuration information (defined and enabled) is displayed. See `cfgshow` for a description of this display.

If a parameter is specified, it is used as a pattern to match QuickLoop names; those that match in the defined configuration are displayed.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands The following operand is optional:

pattern Specify a POSIX style expression used to match QuickLoop names. Patterns may contain the following special characters:

- Question mark `?` that matches any single character
- Asterisk `*` that matches any string of characters
- Ranges `[0-9a-f]` that match any character within the range

qloopremove

Remove a member from a QuickLoop.

Syntax `qloopremove "qloopName", "member;member"`

Availability Admin

This command requires a Zoning license.

Description Use this command to remove one or more members from a QuickLoop.

The member list is identified through an exact string match; therefore, when removing multiple members, order is important. For example, if a QuickLoop contains `"wwn3; wwn4"`, removing `"wwn3; wwn4"` succeeds, but removing `"wwn4; wwn3"` fails.

If all members are removed, the QuickLoop is deleted.

When a configuration is enabled, all QuickLoops defined in the configuration must resolve to one or two switch Worldwide Names.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands The following operands are required:

qloopName	Specify the name of QuickLoop, in quotation marks.
member	Specify the list of QuickLoop members to be removed, in quotation marks, separated by semi-colons. Include one or more of the following: • Worldwide Names • Zone alias names

Example **To remove member "wwn2" from "qlp1":**

```
switch:admin> qloopRemove "qlp1", "wwn2"
```

Example To create two QuickLoops, a single switch and one dual switch:

```
switch:admin> qloopCreate "qlp1", "10:00:00:60:69:00:60:11"
switch:admin> qloopCreate "qlp2", "wwn2; wwn3"
```

See Also
```
qloopadd
qloopdelete
qloopremove
qloopshow
```

qloopdelete

Delete a QuickLoop.

Syntax `qloopdelete "name"`

Availability Admin

This command requires a Zoning license.

Description Use this command to delete a QuickLoop.

This command changes the Defined Configuration. For the change to be preserved across switch reboots, it must be saved to non-volatile memory using the `cfgsave` command. For the change to become effective, an appropriate zone configuration must be enabled using the `cfgenable` command.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands The following operand is required:

name	Specify the name of QuickLoop, in quotation marks. This operand is required.

Example To delete QuickLoop "qloop2":

```
switch:admin> qloopDelete "qloop2"
```

See Also
```
qloopadd
qloopcreate
qloopremove
qloopshow
```

qloopcreate

Create a QuickLoop.

Syntax `qloopcreate "qloopname", "member;member"`

Availability Admin

This command requires a Zoning license.

Description Use this command to create a QuickLoop.

A QuickLoop name must begin with a letter and be followed by any number of letters, digits, and underscore characters. Names are case sensitive, for example `"Qloop_1"` indicates a different QuickLoop than `"qloop_1"`. Blank spaces are ignored.

The QuickLoop member list must have one or two members; an empty list is not allowed.

When a configuration is enabled, all QuickLoops defined in the configuration must resolve to a maximum of two switch Worldwide Names.

Zone alias names entered as members of this QuickLoop must be defined with WWNs. Zone alias names that are defined by domain and port number, or AL_PA are not accepted as members of the QuickLoop.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands The following operands are required:

qloopname Specify the name of QuickLoop to be created, in quotation marks. The qloopname cannot be used for another zone object.

member Specify a list of members to be added to QuickLoop, in quotation marks, separated by semi-colons. Include one or more of the following:

- Worldwide Names
- Zone alias names

qloopadd

Add a member to a QuickLoop.

Syntax `qloopadd "qloopname", "member;member"`

Availability Admin

This command requires a Zoning license.

Description Use this command to add one or more members to an existing QuickLoop.

When a configuration is enabled, all QuickLoops defined in the configuration must resolve to one or two switch Worldwide Names.

Zone alias names entered as members of this QuickLoop must be defined with WWNs. Zone alias names that are defined by domain and port number, or AL_PA are not accepted as members of the QuickLoop.

When security is enabled, this command can only be issued from the Primary FCS switch.

Operands The following operands are required:

qloopname	Specify the name of QuickLoop, in quotation marks.
member	Specify a list of QuickLoop members, in quotation marks, separated by semi-colons. Include one or more of the following: • Worldwide Names • Zone alias names

Example **To add an alias for a second Worldwide Name to "qlp1":**

```
switch:admin> qloopAdd "qlp1", "wwn2"
```

See Also

```
qloopcreate
qloopdelete
qloopremove
qloopshow
```

5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

port Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To view port statistics properties on slot 1 port 3:**

```
switch:admin> ptstatsshow 1/3
Port Statistics for slot: 1, port: 3

Connection type: BE
Configured Speed: 2

Interrupts:      60          Link_failure:       0
Unknown:         2           Loss_of_sync:       0
Lli:             20          Loss_of_sig:        0
Proc_rqrd:       40          Protocol_err:       0
Timed_out:       0           Invalid_word:       0
Rx_flushed:      0           Invalid_crc:        0
Tx_unavail:      0           Delim_err:          0
Free_buffer:     0           Address_err:        0
Overrun:         0           Lr_in:              0
Suspended:       0           Lr_out:             0
Parity_err:      0           Ols_in:             0
2_parity_err:    0           Ols_out:            0
CMI_bus_err:     0
--- <output truncated> ---
```

See Also `portstatsshow`

5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

port — Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example

To display the port routing properties for slot 1 port 3:

```
switch:admin> ptrouteshow 1/3
Port Routing table for slot: 1, port: 3

port address ID: 0x130000
external unicast routing table:
internal unicast routing table:
multicast routing table:
broadcast routing table:
```

See Also

portrouteshow

ptstatsshow

Display port statistics properties.

Syntax

`ptstatsshow [slot/]port`

Availability

All users

Description

Use this command to display the port statistic properties for the specified port.

This command is not intended for normal user operation and is available to provide supplemental information during system debug.

Operands

This command has the following operands:

slot — Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number

Example To display the port registers for slot 1 port 1:

```
switch:admin> ptregshow 1/1
Port Registers for slot: 1, port: 1

0xc9b17000: chip_id         0104        0xc9b17002: port_config    0a38
0xc9b17004: did_vc_map      0800        0xc9b17008: int_mask       064f
0xc9b1700a: int_status      1020        0xc9b1700c: err_status     0003
0xc9b1700e: vc_config       00c0        0xc9b17010: buf_error      00000000
0xc9b17014: mem_bufline     00080008    0xc9b17018: mem_ctl        1024
0xc9b1701a: mem_offset      0000        0xc9b1701c: port_ctl       0000
0xc9b1701e: quad_imask      c003        0xc9b17020: port_addr      00010000
0xc9b17024: lli_status      00040007    0xc9b17028: lli_ctl        00080180
0xc9b1702c: lli_def         00000000    0xc9b17030: lli_mask       00020000
0xc9b17034: prescaler0      000a        0xc9b17036: tod0           0104
0xc9b17038: toc0            0007        0xc9b1703a: toc1           0000
0xc9b1703c: toc_ctl         0000        0xc9b17044: putq_stat      ffffffff
--- <output truncated> ---
```

ptrouteshow

Display port routing properties.

Syntax `ptrouteshow [slot/]port`

Availability All users

Description Use this command to display the ASIC routing table contents.

This command is not intended for normal user operation and is available to provide supplemental information during system debug.

Operands This command has the following operands:

slot Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number

See Also `chippropshow`
`ptregshow`

ptregshow

Display ASIC port registers.

Syntax `ptpropshow [slot/]port`

Availability All users

Description Use this command to display the contents of port registers.

This command is not intended for normal user operation and is available to provide supplemental information during system debug.

Operands This command has the following operands:

slot	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
port	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

ptpropshow

Display port properties.

Syntax `ptpropshow [slot/]port | [slot] -all`

Availability All users

Description Use this command to display the ASIC port properties contents for the specified port.

This command is not intended for normal user operation and is available to provide supplemental information during system debug.

Operands This command has the following operands:

slot	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
port	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.
[*slot*] -all	Specify which slot to operate on. The entire ports in the slot will be displayed. If *slot* is not specified, the current slot will be assumed. This operand is optional.

Example **To display the port properties for slot 1 port 2:**

```
switch:admin> ptpropshow 1/2
Port Property for slot: 1, port: 2

P2: [be,3,2],SP,CAP:[1,1,1,(1,1,0)],WWN: 00:00:00:00:00:00:00:00
```

number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

port Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the port routing tables for slot 2 port 1:**

```
switch:admin> ptphantomshow 2/1
Port Routing table for slot: 2, port: 1

The following alpas are private on some switch ports:
(alpa, UI port bitmap on the blade)

plt_cam table and plt_alpa table:
index      sid                  plt_alpas      ......

plt_did table for this port:
ali  alpa  sid         ali  alpa  sid         ......
```

Example To display the port data structure for slot 1 port 1:

```
switch:admin> ptdatashow 1/1

Port Data Structure for slot: 1, port: 1

Bloom Data Pointers: bloomp = 0xc6eb7200 (fbloomp = 0x00000000)
-------------------
blm_regs           0xc9b17000    blm_proc_dir      0xc50d9f20
fab_ptr            0xc04f0000    fab_Iop           0xc04f0050
qdblm              0xc5702c00    chblm             0xc661b5a0
pt                 0xc5701760    blm_miniS_handle  0xc57012e0

Bloom Local Variables
---------------------
blm_type  = 0x00000012  G_PORT E_PORTto stop
blm_state = 0x00000001  ONLINE  p_phstate = IN_SYNC
blm_flags = 0x00000000  NORMAL
lab_mode  = 0x00        EFD
blm_port_type = Intra-blade     blm_rev           1
blm_initialized   0             my_domain         1
blm_quad_idx      1             blm_chip_idx      1
blm_miniS_idx     1             blm_blade_idx     1
--- <output truncated> ---
```

ptphantomshow

Display the quick-loop CAM tables.

Syntax `ptphantomshow [slot/]port`

Availability All users

Description Use this command to display the quick-loop CAM (Content Addressable Memory) tables.

This command is not intended for normal user operation and is available to provide supplemental information during system debug.

Operands This command has the following operands:

slot Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port

ptdatashow

Display port data structures.

Syntax `ptdatashow [slot/]port`

Availability All users

Description Use this command to display port data structures.

This command is not intended for normal user operation and is available to provide supplemental information during system debug.

Operands This command has the following operands:

slot	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
port	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

psshow

Display power supply status.

Syntax `psshow`

Availability All users

Description Use this command to display the current status of the switch power supplies.

The format of the display varies according to the switch model and number of power supplies present. Optionally, depending upon switch model, the OEM Serial ID Data is displayed after each power supply status line.

The status of each supply is shown as:

OK	Power supply functioning correctly.
absent	Power supply not present.
Unknown	Unknown power supply unit installed.
Predicting Failure	Power supply is present but predicting failure.
faulty	Power supply present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

Operands None

Example **To view the status of the power supply for the current switch:**

```
switch:admin> psshow

Power Supply #1 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0116000747
Power Supply #2 is absent
Power Supply #3 is OK
 DELTA DPS-1001AB-1E 23000000601 S1   IXD0116000757
Power Supply #4 is absent
switch:admin>
```

See Also `fanshow`
`tempshow`

powerofflistshow

Displays slot power off list order.

Syntax `powerofflistshow`

Availability All users

Description Use this command to displays the order in which the physical slots will be powered off. The system available power is compared to the system demand power to determine if there is enough power to operate. If there is less power available than the demand, then the power off list is processed until there is enough power for the system to operate. The format of the display varies depending on the switch model and the number of slots present.

Operands None

Example **To display the slot power off list order:**

```
switch:admin> powerofflistshow

Slot 10 will be powered off 1st
Slot  9 will be powered off 2nd
Slot  8 will be powered off 3rd
Slot  7 will be powered off 4th
Slot  4 will be powered off 5th
Slot  3 will be powered off 6th
Slot  2 will be powered off 7th
Slot  1 will be powered off 8th
switch:admin>
```

See Also

- `powerofflistset`
- `slotpoweron`
- `slotpoweroff`
- `slotshow`
- `chassisshow`
- `psshow`

Example To modify the power off list order:

```
switch:admin> powerofflistset

Slot    Current POL
-------------------
 10         1st
  9         2nd
  8         3rd
  7         4th
  4         5th
  3         6th
  2         7th
  1         8th

1st slot to be power off: (1..10) [10] 7
2nd slot to be power off: (1..10) [9] 8
3rd slot to be power off: (1..10) [9]
4th slot to be power off: (1..10) [10]
5th slot to be power off: (1..4) [4] 1
6th slot to be power off: (2..4) [3] 2
7th slot to be power off: (3..4) [3]
8th slot to be power off: (4..4) [4]

Old POL    New POL    Power Off Order
-----------------------------------
  10          7            1st
   9          8            2nd
   8          9            3rd
   7         10            4th
   4          1            5th
   3          2            6th
   2          3            7th
   1          4            8th

Proceed to change the POL order? (yes, y, no, n): [no] y
switch:admin>
```

See Also powerofflistshow
chassisshow
psshow
slotshow
slotpoweron
slotpoweroff

powerofflistset

Sets slot power off list order.

Syntax `powerofflistset`

Availability Admin

Description Use this command to set the physical power off slot order. The system available power is compared to the system demand power to determine if there is enough power to operate. If there is less power available than the demand, then the power off list is processed until there is enough power for the system to operate. The format of the display varies depending on the switch model and the number of slots present.

When this command is executed, the first item displayed is the current power off list order. Then you are prompted to make any changes, and finally the new power off list order is displayed. The command then prompts to verify and commit the changes.

Operands None

5. Pattern used in testing.
6. Seed used in testing.
7. User Delay value.
8. Total iteration asked to test.
9. Current test iteration.
10. Total Fails on this test.
11. Consecutive Fails on this test.
12. `porttest` Start Time.
13. `porttest` Stop Time.
14. Timeout value.
15. Error code if any.

Options This command has the following option:

`-ports` *`itemlist`* Specify a list of user ports to test. By default all the user ports in the current slot will be assumed. See itemlist help pages for further details.

Example **To display information from `porttest`:**

```
switch:admin> porttestshow 1
     Port 1 : PASS
     PortType: OTHER                    PortState: NO TEST
     PortInternalState: INIT                   PortTypeToTest: NO_TEST
     Pattern: 0x0           Seed: 0x0           UserDelay: 0
     TotalIteration: 0                  CurrentIteration: 0
     TotalFail: 0                       ConsecutiveFail: 0
     StartTime: NONE
     StopTime:  NONE
     Timeout: 0                         ErrorCode: 0
```

See Also

```
porttest
stopporttest
loopporttest
fporttest
crossporttest
portloopbacktest
spinfab
```

`-seed` *seed* Specify the seed pattern to be used with pattern. Default seed value is 0xaa.

`-listtype` *porttype*
Specify the type of ports to run `porttest`. The following values are predefined for *porttype*. The default value is `-1`. Valid values are:

- -1 All ports.
- -2 All L_ports.
- -3 All F_ports.
- -4 All E_ports.
- -5 All Loopback ports.

Example **To run a functional test on an active switch:**

```
switch:admin> porttest -ports 1/1-1/3
```

See Also

```
stopporttest
porttestshow
loopporttest
fporttest
crossporttest
portloopbacktest
spinfab
```

porttestshow

Display information from `porttest`.

Syntax `porttestshow [-ports` *itemlist*`]`

Availability Admin

Description Use this command to display a snapshot of information from `porttest`. The following information is displayed:

1. Pass/Fail information on a given port.
2. Port type tested.
3. Current State of portTest (NO TEST / TESTING / TEST DONE)
4. Type of ports asked to test (ALL_PORTS, ALL_E_PORTS, ALL_L_PORTS, ALL_F_PORTS, ALL_LB_PORTS, or SINGLE_PORT)

Once `porttest` is triggered, you can use `stopporttest` to stop the test. Refer to the `stopporttest` command for more information.

Current progress of `porttest` can be viewed by running `porttestshow`. Refer to the `porttestshow` command for more information.

If there is a port type changes during `porttest` execution, test will continue on a given port as long as it can be supported and it is asked to do so. If a request was made to test all possible ports on a given switch, `porttest` will start a new test using the new port type to start a appropriate test.

Options

This command has the following options:

`-ports` *`itemlist`*
Specify a list of user ports to test. By default all the user ports in the current slot will be assumed. You can set the current slot by issuing setslot command. See itemlist help pages for further details.

`-iteration` *`count`*
Specify the number of times (or number of frames per port) to execute this test. Default value is 20. Valid values are:

0 Run the test on timeout mode.

-1 Run forever.

`-userdelay` *`time`*
Specify the delay between frames sent by `porttest` in minutes. The default value is 10 minutes.

`-timeout` *`time`*
Specify the number of seconds to run the test. Setting the iteration to 0 will set the `porttest` into timeout mode. The default value is 0.

`-pattern`
Specify the pattern of the test packets payload. Default pattern type is RANDOM. Twenty types of predefined patterns are provided with the test. Use the `datatypeshow` command to see the types of pattern that are supported with `porttest`.

`-patsize` *`size`*
Specify the size of the pattern. Default size of the pattern is 1024 bytes. Valid rang of values are 4 bytes through 2112 bytes.

porttest

Functional test of a switch in a live fabric.

Syntax

```
porttest [-ports itemlist] [-iteration count] [-userdelay
time] [-timeout time] [-pattern pattern]
[-patsize size] [-seed seed] [-listtype porttype]
```

Availability

Admin

Description

Use this command to isolate problems to a single replaceable element and isolate problems to near-end terminal equipment, far-end terminal equipment, or transmission line. Diagnostics can be executed every day, and also on demand to troubleshoot a failure.

This command verifies the intended functional operation of the switch by sending frames from port M's transmitter, and looping the frames back via an external fiber cable into port M's receiver; thus exercising all the switch components from the main board to the GBIC to the fiber cable to the SFPs (of the devices and the switch) and back to the main board.

The cables and SFPs connected should be of the same technology: meaning a short wavelength SFP (switch) port is connected to another short wavelength SFP (device) port using a short wavelength cable; and a long wavelength port is connected to a long wavelength port; and a copper port is connected to a copper port.

Only one frame is transmitted and received at any one time. The port LEDs flicker green while the test is running.

The following port types are supported:

- E_ports
- F_ports. (Must support ELS ECHO)
- L_ports
- N->N Loopback ports

This command will not run on any other port type.

The command performs the following actions:

1. Initiate tests on certain ports (`porttest` command)
2. Stop active tests on certain ports (`stopporttest` command)
3. Get the snapshot of the test result. (`porttestshow` command)

```
portenable
portdisable
portswapshow
portswapenable
```

portswapshow

Display information for any ports where area ID numbers have been swapped.

Syntax `portswapshow`

Availability Admin

Description Use this command to displays port and area information for those ports whose area number is different from the default area number. The default area number of a port is same as its switch port number.

Operands None

Example **To display information for port area IDs that have been swapped:**

```
switch:admin> portswapshow
PortSwap is enabled
No ports have been swapped
switch:admin>
```

See Also

```
switchshow
portshow
portenable
portdisable
portswap
portswapenable
portswapdisable
errshow
```

portswapdisable

Disable the portswap feature.

Syntax `portswapdisable`

Availability Admin

Description Use this command to disable the portswap feature. The `portswap` command cannot be used once this feature is disabled.

Operands None

Example **To disable the portswap feature:**

```
switch:admin> portswapdisable
done.
```

See Also
```
switchshow
portshow
portenable
portdisable
portswapshow
portswapenable
```

portswapenable

Enable the portswap feature.

Syntax `portswapenable`

Availability Admin

Description Use this command to enable the portswap feature. The `portswap` command cannot be used unless the feature is first enabled with this command.

Operands None

Example **To enable the portswap feature:**

```
switch:admin> portswapenable
done.
switch:admin>
```

See Also
```
switchshow
portshow
```

portswap

Swap area numbers of two switch ports.

Syntax `portswap [slotnumber/]port1 [slotnumber/]port2`

Availability Admin

Description Use this command to swap area numbers for a pair of switch ports. Both switch ports must be disabled prior to executing this command.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
port1	Specify the port number where you want to swap the area ID number.
port2	Specify the port number where you want to swap the port1 area ID number.

Example **To swap area numbers between a pair of ports:**

```
switch:admin> portswap 1/2 2/5
```

See Also

```
switchshow
portshow
portenable
portdisable
portswapshow
```

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the basic set of statistics for a port:**

```
switch:admin> portstatsshow 7/15
stat_wtx        2528          4-byte words transmitted
stat_wrx        3272          4-byte words received
stat_ftx        104           Frames transmitted
stat_frx        124           Frames received
stat_c2_frx     0             Class 2 frames received
stat_c3_frx     124           Class 3 frames received
stat_lc_rx      0             Link control frames received
stat_mc_rx      0             Multicast frames received
stat_mc_to      0             Multicast timeouts
stat_mc_tx      0             Multicast frames transmitted
tim_rdy_pri     6189438       Time R_RDY high priority
tim_txcrd_z     31            Time BB_credit zero
er_enc_in       0             Encoding errors inside of frames
er_crc          0             Frames with CRC errors
er_trunc        0             Frames shorter than minimum
er_toolong      0             Frames longer than maximum
er_bad_eof      0             Frames with bad end-of-frame
er_enc_out      18            Encoding error outside of frames
er_disc_c3      0             Class 3 frames discarded
open            106           loop_open
transfer        106           loop_transfer
opened          104           FL_Port opened
starve_stop     0             tenancies stopped due to starvation
fl_tenancy      565           number of times FL has the tenancy
nl_tenancy      48            number of times NL has the tenancy
switch:admin>
```

See Also `porterrshow`
`portshow`

`fl_cls_idle`	CLS sent due to loop idle.
`fl_cls_rx`	CLS received when OPEN.
`fl_bb_stall`	OPN/CLS BB_Credit stalls.
`fl_cf_alloc`	Number of CFIFOs allocated.
`fl_cf_opn`	CFIFOs delivered when OPENED.
`fl_cf_full`	Number of CFIFOs full stalls.
`fl_cf_na`	CFIFO not available stalls.
`fl_trig_age`	Number of age count triggers.
`fl_trig_lp`	Number of loop not busy triggers.
`open`	Number of times the FL_Port entered OPEN state.
`transfer`	Number of times the FL_Port entered TRANSFER state.
`opened`	Number of times the FL_Port entered OPENED state.
`starve_stop`	Loop tenancies stopped due to starvation.
`fl_tenancy`	Number of times FL_Port had loop tenancy.
`nl_tenancy`	Number of times NL_Port had loop tenancy.
`frame_nozone`	Frames rejected due to zone protection.

Operands

This command has the following operand:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portstatsshow

Display port hardware statistics.

Syntax `portstatsshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display port hardware statistics counters.

`stat_wtx`	4-byte words transmitted.
`stat_wrx`	4-byte words received.
`stat_ftx`	Frames transmitted.
`stat_frx`	Frames received.
`stat_c2_frx`	Class 2 frames received.
`stat_c3_frx`	Class 3 frames received.
`stat_lc_rx`	Link control frames received.
`stat_mc_rx`	Multicast frames received.
`stat_mc_to`	Multicast timeouts.
`stat_mc_tx`	Multicast frames transmitted.
`tim_rdy_pri`	Time R_RDY high priority.
`tim_txcrd_z`	Time BB_credit zero.
`er_enc_in`	Encoding errors inside frames.
`er_crc`	Frames with CRC errors.
`er_trunc`	Frames shorter than minimum.
`er_toolong`	Frames longer than maximum.
`er_bad_eof`	Frames with bad end-of-frame.
`er_enc_out`	Encoding error outside frames.
`er_disc_c3`	Class 3 frames discarded.
`fl_open`	Number of OPNyx sent.
`fl_opened`	Number of OPNyx received.
`fl_openfr`	Number of OPNfr sent.

See Also `portstatsshow`
`portstatsclear`

portstatsclear

Clear the hardware statistics of a specified switch port.

Syntax `portstatsclear [slotnumber/]portnumber`

Availability Admin

Description Use this command to clear the hardware statistics for a specified switch port. At the same time, this command also clears the hardware statistics for the associated ports in the target port quad.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To clear the hardware statistics for a port:**

```
switch:admin> portstatsclear 8/5
switch:admin>
```

See Also `portstatsshow`

portstats64show

Display the 64-bit hardware statistics for a port.

Syntax `portstats64show [slotnumber/]portnumber`

Availability All users

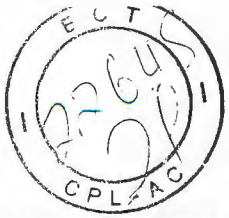
Description Use this command to display the 64-bit hardware statistics for a port.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the 64-bit hardware statistics for a port:**

```
switch:admin> portstats64show 9/1
stat64_wtx      0           top_int : 4-byte words transmitted
                0           bottom_int : 4-byte words transmitted
stat64_wrx      0           top_int : 4-byte words received
                0           bottom_int : 4-byte words received
stat64_ftx      0           top_int : Frames transmitted
                0           bottom_int : Frames transmitted
stat64_frx      0           top_int : Frames received
                0           bottom_int : Frames received
stat64_c2_frx   0           top_int : Class 2 frames received
                0           bottom_int : Class 2 frames received
stat64_c3_frx   0           top_int : Class 3 frames received
                0           bottom_int : Class 3 frames received

--- <output truncated> ---
```



5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the status for a specified E_Port:**

```
switch:admin> portshow 1/5
portName:
portDisableReason: None
portCFlags: 0x1
portFlags: 0xc228057     PRESENT ACTIVE E_PORT G_PORT U_PORT LOGIN LED
   ACCEPT
portType:  4.1
portState: 1    Online
portPhys:  6    In_Sync
portScn:   5    E_Port    Trunk master port,
portId:    010500
portWwn:   20:05:00:60:69:80:03:32
portWwn of device(s) connected:
        None
Distance:  normal
portSpeed: N2Gbps

Interrupts:         1086       Link_failure: 0          Frjt:          0
Unknown:            0          Loss_of_sync: 0          Fbsy:          0
Lli:                0          Loss_of_sig:  0
Proc_rqrd:          1086       Protocol_err: 0
Timed_out:          0          Invalid_word: 0
Rx_flushed:         0          Invalid_crc:  0
Tx_unavail:         0          Delim_err:    0
Free_buffer:        0          Address_err:  0
Overrun:            0          Lr_in:        0
Suspended:          0          Lr_out:       0
Parity_err:         0          Ols_in:       0
2_parity_err:       0          Ols_out:      0
CMI_bus_err:        0

switch:admin>
```

See Also `switchshow`

Table 1-13 portshow Display Fields *(continued)*

Field	Description
Unknown	Interrupts that are not counted elsewhere.
Lli	Low-level interface (physical state, primitive seqs).
Proc_rqrd	Frames delivered for embedded N_Port processing.
Timed_out	Frames that have timed out.
Rx_flushed	Frames requiring translation.
Tx_unavail	Frames returned from an unavailable transmitter.
Free_buffer	Free buffer available interrupts.
Overrun	Buffer overrun interrupts.
Suspended	Transmission suspended interrupts.
Parity_err	Real Tx data parity error.
2ndary_parity_err	Secondary Tx data parity error. These are not real Tx data parity errors but rather forced by the ASIC due to certain central memory errors so that the transmitter will abort the frame. This field will only be displayed when there are errors.
CMI_bus_err	Control message interface errors.

The second column shows Link Error Status Block counters.

The third column shows the number of F_RJTs and F_BSYs generated. For L_Ports, the third column also shows the number of LIPs received, number of LIPs transmitted, and the last LIP received.

Operands This command has the following operand:

`slotnumber` Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number

Table 1-13 portshow Display Fields (*continued*)

Field	Description
portState	Port SNMP state: Online up and running Offline not online, `portPhys` gives details Testing running diagnostics Faulty failed diagnostics
portPhys	Port physical state: No_Card no interface card present No_Module no module (SFP or other) present No_Light module not receiving light No_Sync receiving light but out of sync In_Sync receiving light and in sync Laser_Flt module is signaling a laser fault Port_Flt port marked faulty Diag_Flt port failed diagnostics Lock_Ref locking to the reference signal
portScn	Last state change notification for port.
portId	24-bit D_ID for port.
portWwn	Port WWNs of device(s) connected.
Distance	The port's long distance level.
Speed	The port's fixed speed level or negotiated speed level: 1Gbps - fixed speed of 1 Gbit/sec. N1Gbps - negotiated speed of 1 Gbit/sec. 2Gbps - fixed speed of 2 Gbit/sec. N2Gbps - negotiated speed of 2 Gbit/sec. Negotiating - the speed of the port is being determined.
Interrupts	Total number of interrupts.

```
   7: 0x1 (vc=4)
   8: 0x1 (vc=4)
   9: 0x100 (vc=2)
  10: 0x100 (vc=2)
  11: 0x100 (vc=2)
  12: 0x100 (vc=2)
  14: 0x100 (vc=2)
  15: 0x1 (vc=4)
  16: 0x100 (vc=2)
  17: 0x1 (vc=4)
  18: 0x100 (vc=2)
internal unicast routing table:
  15: 0x1000 (vc=5)
  47: 0x1 (vc=5)
multicast routing table:
broadcast routing table:
   0x10000
switch:admin>
```

See Also

```
bcastshow
fabricshow
mcastshow
switchshow
topologyshow
urouteshow
```

portshow

Display port status.

Syntax `portshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display status information for a port. Information varies with the switch model and port type. The display shows the fields listed in Table 1-13.

Table 1-13 portshow Display Fields

Field	Description
portCFlags	Port control flags.
portFlags	Bit map of port status flags.
portType	Port type and revision numbers.

Multicast routing table	Displays multicast frame routing to the destination multicast group. Output format is:
	`mcast_group_number: (mcast_group_id) ports_bitmap`
	where
	`mcast_group_number` is the multicast group number
	`mcast_group_id` is the multicast frame destination ID
	`ports_bitmap` is a hex bitmap of all output port numbers that can forward a multicast frame from the `portnumber` to `mcast_group_id`

Broadcast routing table	A bitmap, containing all ports reachable by a received broadcast frame. Bit 16 of the bitmap is always set to allow the switch element to receive broadcast frames.

Operands This command has the following operand:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15). The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.
portnumber	Specify a port number. Valid values for port number vary depending on the switch type. This operand is required.

Example **To display the routing tables for a port:**

```
switch:admin> portrouteshow 7/15
port address ID: 0x030f00
external unicast routing table:
   1: 0x100 (vc=2)
   2: 0x100 (vc=2)
   3: 0x10000 (vc=0)
   4: 0x100 (vc=2)
   5: 0x1 (vc=4)
   6: 0x1 (vc=4)
```

portrouteshow

Display routing tables for a port.

Syntax `portrouteshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display the port address ID and the contents of the following port routing tables:

External unicast routing table — Displays unicast frame routing to another switch element in the fabric. Output format is

```
domain_number: ports_bitmap
```

where:

`domain_number` is the switch element number that a unicast frame can reach from the `portnumber` port.

`ports_bitmap` contains all output ports, in bitmap hex format, that can forward unicast frames from port number to domain number.

This table contains at least one entry for each active port:

```
local_switch_domain_number: 0x10000
```

This is for routing unicast frames designated to the embedded port of the local switch element.

Internal unicast routing table — Lists all ports in the local switch that a unicast frame can reach from portnumber. Format is

```
destination_port: output_ports_bitmap
```

Because the `destination_port` is in the local switch, `output_ports_bitmap` usually contains one bit with a bit position number representing the `destination_port` number.

`-slot` *number*	Specify the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is 0.
`-ports` *itemlist*	Specify a list of blade ports to test. By default all the blade ports in the specified slot will be used. See `itemlist` help pages for further details.
`-skiptests` *mask*	A bit mask that defines which of the register test subtests to skip. By default, all subtests will be performed. Valid mask values include one or more of the following:

Value	Description
0x2	Skip retry register test.
0x4	Skip statistics register test.
0x8	Skip walk-1 test.
0x10	Skip credit counter test.

`-verbose` *mode*	Specify a non-zero value to enable verbose mode. The default value is to disable this mode.

Example **To run a bit write/read test of the ASIC SRAMs and registers:**

```
switch:admin> portregtest -ports 1/0-1/15
Running Port Register Test ....
Test Complete: "portregtest" Pass 1 of 1
Duration 0 hr, 0 min & 33 sec (0:0:33:447).
passed.
```

Errors When this command detects failure(s), the test may report one or more of the following error messages:

```
BUS_TIMEOUT
REGERR
REGERR_UNRST
```

See Also

```
camtest
centralmemorytest
cmemretentiontest
cmitest
crossporttest
itemlist
portloopbacktest
spinsilk
sramretentiontest
```

Example To display port throughput for a switch:

```
switch:admin> portperfshow
   0    1    2    3    4    5    6    7    8    9   10   11   12   13   14   15
 Total
==========================================================================
========
   0    0    0    0    0    0    0    0    0    0    0  408    0    0    0    0

  16   17   18   19   20   21   22   23   24   25   26   27   28   29   30   31
==========================================================================
========
   0    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
 408
```

See Also `portstatsshow`

portregtest

Read and write test of the ASIC SRAMs and registers.

Syntax `portregtest [-slot` *number*`] [-ports` *itemlist*`] [-skiptests` *mask*`] [-verbose mode]`

Availability Admin

Description Use this command to verify that SRAM and register data bits in each ASIC can be independently written and read.

The test method used is to write a walking 1 pattern to each bit location. This is done by writing a pattern of 0x00000001 to register N, read and make sure that the same pattern previously written is read back. Shift the pattern to the left by 1 bit (to 0x00000002), repeat the write, read and compare cycle. Shift again and repeat until the last writable bit in register N is reached (0x80000000 for a 32-bit register).

For example a 6-bit register is effectively tested with the following patterns:

```
0x0001    0x0002    0x0004    0x0008
0x0010    0x0020    0x0040    0x0080
0x0100    0x0200    0x0400    0x0800
0x1000    0x2000    0x4000    0x8000
```

Repeat the above steps until all ASIC SRAMs and registers are tested.

Operands This command has the following operands:

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

portname Specify a port name. The port name is a character string from 1 to 32 characters. This operand must be enclosed in quotation marks. This operand is optional.

Example

To name to a port:

```
switch:admin> portname 1/3, "Tape drive 5"
Committing configuration...done.
Tape drive 5
switch:admin> portname 1/3
Tape drive 5
```

See Also

```
portshow
configdefault
portcfgdefault
```

portperfshow

Display port throughput performance in bytes, kilobytes, or megabytes.

Syntax

```
portperfshow [interval]
```

Availability

All users

Description

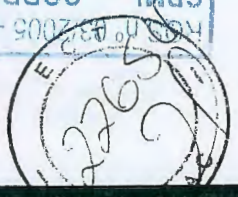
Use this command to display throughput information for all ports on the switch (8 or 16 columns depending on the switch model). One output line is displayed per interval (or second if no interval is specified) until RETURN, CTRL-C, or CTRL-D is entered.

This command displays the number of bytes received plus the number of bytes transmitted per interval. Throughput values are dislayed as either bytes, kilobytes (k), or megabytes (m).

Operands

This command has the following operand:

interval Specify the interval, in seconds, between each sample. This operand is optional.



portname

Assign or display a port name.

Syntax `portname [slotnumber/]portnumber, "portname"`

Availability Admin

Description Use this command to assign or display a port name. Both *port_number* and *port_name* operands are optional for this command.

With both the operands present, the port name string will be assigned to the port. With only the port name operand, the previously assigned port name will be displayed. With no operands, the port names of all the ports present will be displayed.

The port name is a string of length 32 characters or less. It may consist of white spaces or printable characters, excluding the characters comma and semi-colon. By default, a port has no name until it is explicitly assigned by the user.

A null string (that is no *port_name* specified) is used as the default port name when a port had no user assigned name. A port name can be reset to the default value by executing the `portname` command with the second operand as a null string.

Like all other configurable port attributes, port name will be persistent across reboots and power cycles. It will not be affected by `configdefault` command but it will be cleared by `portcfgdefault`.

Operands This command has the following operand:

slotnumber Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

- 6: set all odd ports' speed for auto-negotiate, set all even ports' speed for 2 Gbit/sec.

For `lbMode==` 2,3 the following speed modes are available to test fifo underrun.

- 3,5: set all even ports' speed for 2 Gbit/sec, set all odd ports' speed for 1 Gbit/sec.
- 4,6: set all even ports' speed for 1 Gbit/sec, set all odd ports' speed for 2 Gbit/sec.

`-ports` *`itemlist`* Specify a list of user ports to test. By default all of the user ports in the current switch are tested. This option may be used to restrict testing to the specified ports.

Example **To run a functional test of a connection:**

```
switch:admin> portloopbacktest -ports 1/38-1/45 -nframes 1 -lb_mode 1
Running Port Loopback Test ....
passed.
```

Errors Below are possible error messages if failures are detected:

```
DATA
ERRSTAT
INIT
PORTDIED
STATS
TIMEOUT
XMIT
```

See Also

```
camtest
centralmemorytest
cmemretentiontest
cmitest
crossporttest
itemlist
portregtest
ramtest
spinsilk
sramretentiontest
```

`-slot number` — Specify the slot number that the diagnostic will operate on. The ports specified will be relative to this slot number. The default is set to 0 and designed to operate on fixed port count products.

`-nframes count` — Specify the number of frames to send. The test will progress until the specified number of frames has been transmitted on each port. The default value is 10.

`-lb_mode mode` — Specify the loopback mode for the test. By default, this test uses internal loopback. Valid values are as follows:

1 Port Loopback (loopback plugs)

2 External (SERDES) loopback

5 Internal (parallel) loopback

`-spd_mode mode` — Specify the speed mode for the test. For 1 Gbit/sec only products it is ignored. The exact operation of modes 3 through 6 depends upon the loopback mode selected. When speed modes 3 through 6 are used with cables, they must be connected EVEN to ODD or the test will fail.

- 0: set all ports' speed for auto-negotiate.
- 1: set all ports' speed to lock at 1 Gbit/sec.
- 2: set all port's speed to lock at 2 Gbit/sec.
- For `lb_mode` == 0,1 the following speed modes are available to test the speed negotiation:
- 3: set all even ports' speed for auto-negotiate, set all odd ports' speed for 1 Gbit/sec.
- 4: set all even ports' speed for auto-negotiate, set all odd ports' speed for 2 Gbit/sec.
- 5: set all odd ports' speed for auto-negotiate, set all even ports' speed for 1 Gbit/sec.

Below is the test method:

1. Set all ports for parallel loopback.
2. Create a frame F of maximum data size (2112 bytes).
3. Transmit frame F through port N.
4. Pick up the frame from the same port N.
5. Check the 8 statistic error counters for nonzero values:

   ```
   ENC_in, CRC_err, TruncFrm, FrmTooLong, BadEOF,
      Enc_out, BadOrdSet, DiscC3.
   ```

6. Check if the transmit, receive or class 3 receiver counters are stuck at some value.
7. Check if the number of frames transmitted is not equal to the number of frames received.
8. Repeat steps 2 through 7 for all ports present until:

   - The number of frames (or *passcount*) requested is reached.

   - All ports are marked bad.

At each pass, the frame is created from a different data type. If seven passes are requested, seven different data types are used in the test. If eight passes are requested, the first seven frames use unique data types, and the eighth is the same as the first. The seven data types are:

```
1) CSPAT: 0x7e, 0x7e, 0x7e, 0x7e, ...
2) BYTE_LFSR: 0x69, 0x01, 0x02, 0x05, ...
3) CHALF_SQ: 0x4a, 0x4a, 0x4a, 0x4a, ...
4) QUAD_NOT: 0x00, 0xff, 0x00, 0xff, ...
5) CQTR_SQ: 0x78, 0x78, 0x78, 0x78, ...
6) CRPAT: 0xbc, 0xbc, 0x23, 0x47, ...
7) RANDOM: 0x25, 0x7f, 0x6e, 0x9a, ...
```

Since this test does not include the media or the fiber cable in its test path, its results combined with the results of `crossporttest` and `spinsilk` (both of which loop frames using an external loopback cable) can be used to determine which components of the switch are faulty.

Operands This command has the following operand:

```
portlogeventshow
```

portlogtypeenable

Enable the port log of specified portlog type.

Syntax `portlogtypeenable` *type*

Availability Admin

Description Use this command to enable the portlog for a specified portlog type.

Operands This command has the following operands:

type	Specify a nonzero value that corresponds to the portlog type to be enabled. The values corresponding to different log types can be obtained by running `portlogeventshow`.

Example Enable event 2 to report to the portlog:

```
switch:admin> portlogtypeenable 2
```

See Also

```
portlogdisable
portlogtypeenable
portlogeventshow
```

portloopbacktest

Functional test of port N->N path.

Syntax `portloopbacktest [--slot` *number*`] [-nframes` *count*`] [-lb_mode` *mode*`] [-spd_mode` *mode*`] [-ports` *itemlist*`]`

Availability Admin

Description Use this command to verify the functional operation of the switch by sending frames from the port N transmitter, and looping the frames back into the same port N receiver. The loopback is done at the parallel loopback path. The path exercised in this test does not include the media or the fiber cable.

Only one frame is transmitted and received at any one time. No external cable is required to run this test. The port LEDs flicker green rapidly while the test is running.

Example The following example shows a section of the port log with an E_Port coming online. The ELP and EFP exchanges are shown; a name service request was processed.

```
switch:admin> portlogshowport 24
time          task       event  port cmd  args
-----------------------------------------------
18:24:25.648  PORT       debug   59      ccca0000,0000002c,0000001f,00000000
08:35:27.899  tReceive    pstate  14  LR2
08:35:27.916  tReceive    pstate  14   AC
08:35:28.416  interrupt   scn     14    1
08:35:28.433  tFabric     ioctl   14   90  101d9910,0
08:35:28.433  tFabric     Tx      14  164
   02fffffd,00fffffd,0005ffff,10000000
08:35:28.433  tReceive    Rx      14    0  c0fffffd,00fffffd,00050006
08:35:28.433  tReceive    Rx      14  164
   03fffffd,00fffffd,00050006,02000000

--- <output truncated> ---
```

See Also
```
portlogclear
portlogshow
uptime
```

portlogtypedisable

Disable the port log of specified portlog type.

Syntax `portlogtypedisable` *type*

Availability Admin

Description Use this command to disable the portlog for a specified portlog type.

Operands This command has the following operands:

type	Specify a nonzero value that corresponds to the portlog type to be disabled. The values corresponding to different log types can be obtained by running `portlogeventshow`.

Example **To disable event 2 from reported to the portlog:**

```
switch:admin> portlogtypedisable 2
```

See Also
```
portlogdisable
portlogtypeenable
```

```
portlogdump
uptime
```

portlogshowport

Display the port log of specified port, with page breaks.

Syntax `portlogshowport [portid]`

Availability All users

Description Use this command to display the port log, showing 22 entries at a time. It is identical to `portlogdumpport`, except that `portlogdumpport` does not prompts the user to type return between each page of output.

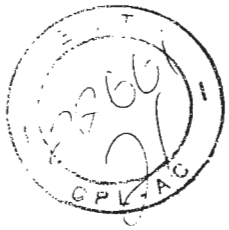
If the port log is disabled, the following message is printed as the first line (see `portlogclear` for details):

```
WARNING: port log is disabled
```

Refer to the `portlogdump` command for more information on the data returned by this command.

Operands This command has the following operands:

portid	Specify a non-zero value that specifies which port will be displayed.



Operands This command has the following operands:

count	Specify the maximum number of lines to display. Only the most recent count entries are displayed. This operand is optional.
saved	Specify a non-zero value to display the saved port log from the last switch fault. See uptime for a list of conditions that cause a fault. count is ignored when displaying the saved log. This operand is optional.
portid	Specify the area number of port to be displayed. If a port area number is specified, all other ports on the switch are ignored. This operand is optional.

Example **To view the port log for a port:**

```
switch:admin> portlogdump 26
time          task       event   port cmd  args
-----------------------------------------------
16:56:25.588  PORT       debug   26       00c0ffee,00fd0188,00000000,00000001
16:56:35.470  PORT       Tx      26   40  02ffffd,00fffffd,0045ffff,14000000
16:56:35.480  PORT       debug   26       00c0ffee,00fd018a,14000000,00000001
16:56:35.491  PORT       debug   26       aaaaaaaa,00140000,00000000,00000000
16:56:35.491  PORT       debug   26       beb01020,00000186,00000000,ffffffff
16:56:35.492  PORT       Rx      26    0  c0fffffd,00fffffd,00450045
16:56:45.592  PORT       debug   26       aaaaaaaa,00140000,00000000,00000000
16:56:45.592  PORT       debug   26       beb01020,0000018c,00000000,ffffffff
16:56:45.592  PORT       Rx      26   40  02ffffd,00fffffd,0046ffff,14000000
16:56:45.592  PORT       Tx      26    0  c0fffffd,00fffffd,00460046
16:56:45.593  PORT       debug   26       00c0ffee,00fd0190,00000000,00000001
16:56:55.471  PORT       Tx      26   40  02ffffd,00fffffd,0047ffff,14000000
16:56:55.471  PORT       debug   26       00c0ffee,00fd0192,14000000,00000001
16:56:55.473  PORT       debug   26       aaaaaaaa,00140000,00000000,00000000
16:56:55.473  PORT       debug   26       beb01020,0000018e,00000000,ffffffff
16:56:55.473  PORT       Rx      26    0  c0fffffd,00fffffd,00470047
16:57:03.282  PORT       Tx      26  204  02fffc02,00fffc61,0048ffff,01000000
16:57:03.283  PORT       debug   26       00c0ffee,00020196,01000000,00000001
16:57:03.284  PORT       debug   26       aaaaaaaa,00140000,00000000,00000000
16:57:03.284  PORT       debug   26       beb01020,00000194,00000000,ffffffff
16:57:03.284  PORT       Rx      26    0  c0fffc61,00fffc02,00480048
16:57:05.557  PORT       debug   26       aaaaaaaa,00140000,00000000,00000000
16:57:05.557  PORT       debug   26       beb01020,00000198,00000000,ffffffff
16:57:05.557  PORT       Rx      26   40  02ffffd,00fffffd,0049ffff,14000000
16:57:05.558  PORT       Tx      26    0  c0fffffd,00fffffd,00490049
16:57:05.558  PORT       debug   26       00c0ffee,00fd019c,00000001,01000001

switch:admin>
```

See Also portlogclear

portlogshow

Display the port log.

Syntax `portlogshow [count, saved, portid]`

Availability All users

Description Use this command to display the port log. This command displays 22 entries at a time.

The `portlogshow` command displays the same information as `portlogdump`, but it enables you to enter a "return" after each page of output.

Port logs are circular log files in the switch firmware, which can save up to 8000 entries per logical switch in v4.1. Once the log is full, the newest log entries delete the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device-to-device1 and control information.

If the port log is disabled, the following message appears as the first line. Refer to `portlogclear` command for more information.

```
WARNING: port log is disabled
```

The following information is displayed for each log entry;

Time	Displays the event date and time in milliseconds.
Task	Displays the name of the internal switch procedure that logged the event.
Event	Displays the task event that generated log entry.
Port #	Displays the Port number that logged the event.
Cmd	Defined by the event. Refer to the *Fabric OS Procedures Guide* for more information.
Args	Displays more information about the event. For ioctl events, these are the I/O control arguments For Tx and Rx, these are the first two header words and word four of the FC-PH frame along with the first word of the payload and internal decoding field.

For a full explanation of the information displayed by this command refer to the *Fabric OS Procedures Guide*.

portlogreset

Enable the portlog facility.

Syntax `portlogreset`

availability Admin

Description Use this command to enable the portlog facility.

Operands None

Example **To enable the portlog:**

```
switch:admin> portlogreset
```

See Also `portlogdisable`

portlogresize

Resize the port log to the specified number of entries.

Syntax `portlogresize` *num_entries*

availability Admin

Description Use this command to resize the port log to specified number of entries. If *num_entries* is less than the already configured port log size, no change is effected.

Operands This command has the following operands:

num_entries	Specify the number of entries to which portlog needs to resized. Valid range of values are 8192 to 16384.

Operands None

Example **To resize the portlog:**

```
switch:admin> portlogresize 10000
```

See Also `portlogconfigshow`

The ED-12000B has a total of 1 - 10 slots. Slot number 5 and 6 are control processor cards, and slot 1 through 4 and 7 through 10 are port cards. On each port card, there are 16 ports counted from the bottom 0 to 15.

portnumber Specify a port number. Valid values for port number vary depending on the switch type. This operand is optional.

Example The following example shows an N_Port with one FLOGI and two PLOGIs:

```
switch:admin> portloginshow 23
Type  PID     World Wide Name         credit df_sz cos
=====================================================
fe  201700  21:00:00:e0:8b:05:a3:c9      3  2048   8  scr=1
ff  201700  21:00:00:e0:8b:05:a3:c9      0     0   8  d_id=FFFC20
ff  201700  21:00:00:e0:8b:05:a3:c9      0     0   8  d_id=FFFFFC
```

See Also `portshow`
`fcpprobeshow`

portlogpdisc

Set or clear the debug_pdisc_flag.

Syntax `portlogpdisc lvl`

Availability Admin

Description Use this command to set or clear the debug_pdisc_flag.

Operands This command has the following operand:

lvl Specify either 0 to clear the flag or 1 to set the pdisc_flag.

Example **To set the pdisc_flag:**

```
switch:admin> portlogpdisc 1
PDISC log setting = 1
```

portloginshow

Display port logins.

Syntax `portloginshow [slotnumber/]portnumber`

Availability All users

Description Use this command to display port login information. Some information varies with the switch model and port type. The lines of the display show:

Type	Type of login: fe FLOGI, Fabric Login to Fabric F_Port. ff PLOGI, Process Login to specific N- Ports or well-known address like Name Server. fd FDISC, Virtual N_Port login.
PID	The port's 24-bit D_ID.
WWN	The port's Worldwide Name.
credit	The credit for this login as appropriate, this is BB (Buffer to Buffer) Credit for FLOGIs and EE (End to End) Credit for PLOGIs.
df_sz	The default frame size for this login.
cos	Class of Services supported. This can be a combination of the following bits. 8 Class of Service includes class 2. 10 Class of Service includes class 3.

There is further information about the login after the above columns. This can include the DID (Destination Identifier) that the port is logged on to.

Operands This command has the following operands:

slotnumber	Specify the slot number for a ED-12000B switch. For all other switches this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

Example To display information about portlog events:

```
switch:admin> portlogeventshow
ID      Event-Name      Disabled
---------------------------------
1       start           0
2       disable         0
3       enable          0
4       ioctl           0
5       Tx              0
6       Tx1             0
7       Tx2             0
8       Tx3             0
9       Rx              0
10      Rx1             0
11      Rx2             0
12      Rx3             0
13      stats           0
14      scn             0
15      pstate          0
16      reject          0
17      busy            0
18      ctin            0
19      ctout           0
20      errlog          0
21      loopscn         0
22      create          0
23      debug           1
24      nbrfsm          0
25      timer           0
26      sn              0
27      fcin            0
28      fcout           0
29      read            0
30      write           0
31      err             0
32      frame           0
33      msRemQ          0
34      msRemR          0
35      nsRemQ          0
36      nsRemR          0
37      rscn            0
38      state           0
39      xalloc          0
40      xfree           0
```

See Also portlogtypeenable
portlogtypedisable

Example To display the port log dump for a port:

```
switch:admin> portlogdumpport 5
time          task       event   port cmd  args
-----------------------------------------------
16:43:35.963  PORT       Rx       5   40  02fffffd,00fffffd,0a3bffff,14000000
16:43:35.963  PORT        Tx       5    0  c0fffffd,00fffffd,0a3b0536
16:43:35.967  PORT       Tx       5   40  02fffffd,00fffffd,0537ffff,14000000
16:43:35.970  PORT        Rx       5    0  c0fffffd,00fffffd,05370a3c
16:43:55.974  PORT       Rx       5   40  02fffffd,00fffffd,0a3fffff,14000000
16:43:55.974  PORT        Tx       5    0  c0fffffd,00fffffd,0a3f053a
16:43:55.978  PORT       Tx       5   40  02fffffd,00fffffd,053bffff,14000000
16:43:55.980  PORT        Rx       5    0  c0fffffd,00fffffd,053b0a40
16:43:57.772  PORT       Tx       5   20  02fffc08,00fffc04,053cffff,01000000
16:43:57.776  PORT        Rx       5    0  c0fffc04,00fffc08,053c002a
16:43:57.781  PORT       Rx       5  132  03fffc04,00fffc08,053c002a,01000000
switch:admin>
```

See Also `portlogclear`
`portlogshow`
`uptime`

portlogeventshow

Display information about portlog events.

Syntax `portlogeventshow`

Availability Admin

Description Use this command to display information about the ID associated with the various port log events and whether the events are enabled or disabled.

Operands None

switch-to-device, device-to-switch, switch-to-switch, some device-to-device1 and control information.

If the port log is disabled, the following message appears as the first line. Refer to `portlogclear` command for more information.

```
WARNING: port log is disabled
```

The following information is displayed for each log entry;

Time	Displays the event date and time in milliseconds.
Task	Displays the name of the internal switch procedure that logged the event.
Event	Displays the task event that generated log entry.
Port #	Displays the Port number that logged the event.
Cmd	Defined by the event. Refer to the *Fabric OS Procedures Guide* for more information.
Args	Displays more information about the event. For ioctl events, these are the I/O control arguments For Tx and Rx, these are the first two header words and word four of the FC-PH frame along with the first word of the payload and internal decoding field.

For a full explanation of the information displayed by this command refer to the *Fabric OS Procedures Guide*.

Operands This command has the following operand:

portid	Specify the area number of port to be displayed. If a port area number is specified, all other ports on the switch are ignored. This operand is optional.

count	Specify the maximum number of lines to be displayed. Only the most recent *count* entries are displayed. This operand is optional.
saved	Specify a nonzero value to display the saved port log from the last switch fault. See **uptime** for conditions that cause a fault. The operand *count* is ignored when displaying the saved log. This operand is optional.
portid	Specify the port to be displayed. All other ports will not be displayed. This operand is optional.

Example **To display the port log for a port:**

```
switch:admin> portlogdump 41
time          task       event  port cmd  args
-----------------------------------------------
16:44:21.490  PORT       Rx     41   40   02fffffd,00fffffd,0005ffff,14000000
16:44:21.490  PORT        Tx     41    0   c0fffffd,00fffffd,00050541
16:44:32.503  PORT       Tx     41   40   02fffffd,00fffffd,0542ffff,14000000
16:44:32.506  PORT        Rx     41    0   c0fffffd,00fffffd,05420006
16:44:42.340  PORT       Rx     41   40   02fffffd,00fffffd,0009ffff,14000000
16:44:42.340  PORT        Tx     41    0   c0fffffd,00fffffd,00090545

--- <output truncated> ---
```

See Also `portlogclear`
`portlogshow`
`uptime`

portlogdumpport

Display the port log of specified port, without page breaks.

Syntax `portlogdumpport` *portid*

Availability All users

Description Use this command to display the port log of specified port. The command displays all entries in the log without any page breaks. It is identical to `portlogshowport`, except that `portlogshowport` prompts the user to type return between each page of output.

Port logs are circular log files in the switch firmware, which can save up to 8000 entries per logical switch in v4.1. Once the log is full, the newest log entries delete the oldest log entries. Port logs capture

portlogdump

Display the port log without page breaks.

Syntax `portlogdump [count[, saved[, portid]]]`

Availability All users

Description Use this command to display the port log, listing all entries in the log without page breaks. This command displays the same information as `portlogshow`, but `portlogshow` prompts the user to enter "returns" between each page.

Port logs are circular log files in the switch firmware, which can save up to 8000 entries per logical switch in v4.1. Once the log is full, the newest log entries delete the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device-to-device1 and control information.

If the port log is disabled, the following message appears as the first line. Refer to `portlogclear` command for more information.

```
WARNING: port log is disabled
```

The following information is displayed for each log entry;

Time	Displays the event date and time in milliseconds.
Task	Displays the name of the internal switch procedure that logged the event.
Event	Displays the task event that generated log entry.
Port #	Displays the Port number that logged the event.
Cmd	Defined by the event. Refer to the *Fabric OS Procedures Guide* for more information.
Args	Displays more information about the event. For ioctl events, these are the I/O control arguments For Tx and Rx, these are the first two header words and word four of the FC-PH frame along with the first word of the payload and internal decoding field.

For a full explanation of the information displayed by this command refer to the *Fabric OS Procedures Guide*.

Operands This command has the following operands:

portlogclear

Clear the port log.

Syntax `portlogclear`

Availability Admin

Description Use this command to clear the port log. You may want to clear the port log before triggering an activity so that the log displays only the activity related to that activity.

If the port log is disabled, the following message appears as the first line.

```
WARNING: port log is disabled
```

If the port log is disabled, `portlogclear` enables it. Certain errors automatically disable the port log to preserve information needed to understand the error (new events are not collected so that existing information is not over-written).

Operands None

Example **To clear the port log:**

```
switch:admin> portlogclear
switch:admin> portlogshow
port log is empty
switch:admin>
```

Errors The following errors disable the port log:

```
FCIU, IUBAD
FCIU, IUCOUNT
FCPH, EXCHBAD
FCPH, EXCHFREE
NBFSM, DUPEPORTSCN
UCAST, RELICPDB
```

See Also

```
portlogdump
portlogshow
```

portledtest

Cycle user port LEDs

Syntax `portledtest [-npass count] [-ports itemlist]`

Availability Admin

Description Use this command to exercise the user port LEDs in the current switch ON/OFF by setting the ATTN LEDs to green for the ON condition and black for the OFF condition. The SPEED LEDs are initially set to black before the command execution. The SPEED LEDs are set to green once the command is executing.

You must disable the current switch (using the `switchdisable` command) before running this command. After the command had completed, the ATTN LEDs flash amber indicating the command has finished and exited. You can enable the current switch (using the `switchenable` command) to set the ATTN LEDs back to black.

Options This command has the following operands:

`-npass count`	Specify the number of times to perform this test. The default value is 10.
`-ports itemlist`	Specify a list of user ports to run the test. If omitted, all the active ports in the switch are assumed. For more information refer to the `itemlist` command.

Examples **To test port LEDs:**

```
switch:admin> portledtest -ports 1/1-1/5
passed.
switch:admin>
```

See Also

```
itemlist
ledtest
switchdisable
switchenable
```


```
switch:user> portflagsshow
Slot  Port    SNMP              Physical        Flags
--------------------------------------------------------
1       0     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       1     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       2     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       3     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       4     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       5     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       6     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       7     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1       8     Offline           No_Light        PRESENT LED
1       9     Offline           No_Light        PRESENT LED
1      10     Offline           No_Light        PRESENT LED
1      11     Offline           No_Light        PRESENT LED
1      12     Online            In_Sync         PRESENT ACTIVE E_P
ORT G_PORT LOGIN LED ACCEPT
1      13     Online            In_Sync         PRESENT ACTIVE E_P

--- <output truncated> ---
```

See Also `portshow`
`portstatsshow`

portflagsshow

Display the port status bitmaps for all ports in a switch

Syntax `portflagsshow`

Availability All users

description Use this command to display the following status for a port:

SNMP	Displays whether the port is online or offline.
Physical	Displays the port physical status. Valid values are In_Sync and No_Light.
Flags	Displays whether there is a SFP inserted in the port, whether the port is active, and the port type.

Operands None

Example To display the port status for all ports in the switch:

loss sync	Loss of synchronization.
loss sig	Loss of signal.
frjt	Frames rejected with F_RJT.
fbsy	Frames busied with F_BSY.

Operands None

Example **To display error counters for ports on a switch:**

```
switch:admin> porterrshow
        frames   enc  crc  too  too  bad  enc disc link loss loss frjt fbsy
       tx    rx   in  err shrt long  eof  out   c3 fail sync
   sig=====================================================================
  0:   22    24    0    0    0    0    0 1.5m    0    7    3    0    0    0
  1:   22    24    0    0    0    0    0 1.2m    0    7    3    0    0    0
  2:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
  3:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
  4: 149m   99m    0    0    0    0    0  448    0    7    6    0    0    0
  5: 149m   99m    0    0    0    0    0  395    0    7    6    0    0    0
  6: 147m   99m    0    0    0    0    0  706    0    7    6    0    0    0
  7: 150m   99m    0    0    0    0    0  160    0    7    5    0    0    0
  8:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
  9:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 10:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 11:    0     0    0    0    0    0    0    0    0    0    0    2    0    0
 12:    0     0    0    0    0    0    0    0    0    0    0    2    0    0
 13:    0     0    0    0    0    0    0    0    0    0    0    2    0    0
 14:    0     0    0    0    0    0    0    0    0    0    0    2    0    0
 15:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 32:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 33:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 34:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 35:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 36:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 37:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 38:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 39:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 40:  99m  146m    0    0    0    0    0  666    0    6  796    7    0    0
 41:  99m  149m    0    0    0    0    0  15k    0    2  303    4    0    0
 42:  99m  152m    0    0    0    0    0  665    0    2  221    5    0    0
 43:  99m  147m    0    0    0    0    0  16k    0    2  144    4    0    0
 44:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 45:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
 46:    0     0    0    0    0    0    0    0    0    0    0    2    0    0
 47:    0     0    0    0    0    0    0    0    0    0    0    0    0    0
switch:admin>
```

Related Documentation

Related product information can be found in the following EMC publications:

- *EMC Connectrix B Series Diagnostic and System Error Message Reference Manual*
- *EMC Connectrix B Series Fabric Watch Reference Manual*
- *EMC Connectrix B Series Management Information Base (MIB) Reference Manual*
- *EMC Connectrix B Series Zoning Reference Manual*
- *EMC Connectrix B Series Extended Fabrics User Guide*
- *EMC Connectrix B Series Interswitch Link (ISL) Trunking User Guide*
- *EMC Connectrix B Series Performance Monitoring User Guide*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Procedures Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 and Enterprise Director Model ED-12000B Web Tools User Guide*
- *EMC Connectrix Enterprise Director ED-12000B Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-32B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Hardware Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Reference Manual*
- *EMC Connectrix Departmental Switch DS-16B2 Web Tools User Guide*
- *EMC Connectrix Departmental Switch DS-16B2 Fabric OS Procedures Manual*

Conventions Used in This Guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

Typographical Conventions

EMC uses the following type style conventions in this guide:

AVANT GARDE	Keystrokes
Palatino, bold	◆ Dialog box, button, icon, and menu items in text ◆ Selections you can make from the user interface, including buttons, icons, options, and field names
Palatino, italic	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
`Courier, italic`	Arguments used in examples of command line syntax.

`Courier`	System prompts and displays and specific filenames or complete paths. For example:
	`working root directory [/user/emc]:`
	`c:\Program Files\EMC\Symapi\db`

`Courier, bold`	◆ User entry. For example: **`symmpoll -p`** ◆ Options in command line syntax

MVS Type Conventions

The syntax conventions used in this guide are:

- CAPITALIZATION = must be typed
- { } = required entry

- [ ] = optional entry
- | = alternative parameter value
- UNDERSCORED = default value or menu selection

Where to Get Help

For questions about technical support, call your local sales office or service provider.

For Symmetrix or CLARiiON Products

If you have a valid EMC service contract, contact EMC Customer Service at:

United States:	**(800) 782-4362 (SVC-4EMC)**
Canada:	**(800) 543-4782 (543-4SVC)**
Worldwide:	**(508) 497-7901**

Follow the voice menu prompts to open a service call and select the applicable product support.

If you are located outside North America, call the nearest EMC office for technical assistance.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

http://www.EMC.com/contact/

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

http://powerlink.EMC.com

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send a message to **techpub_comments@EMC.com** with your opinions of this guide.

1 Introduction

This chapter includes the following sections:

Introduction

Connectrix B Fabric Manager (also called Fabric Manager) lets you manage your EMC Connectrix B-Series and Brocade-based storage area networks (SAN) from a single user interface. With this software, you can configure any aspect of your SAN. Fabric Manager encompasses multiple fabrics, all Connectrix B-Series and Brocade-based switch types, and all Fabric OS firmware versions.

Use Fabric Manager to configure multiple switches simultaneously from one location. View the status of multiple devices in one window. Perform SAN-level maintenance without accessing switch after switch. Fabric Manager lets you administer all of the elements of your SAN from one point of entry.

All switches in the fabric are represented in the main window of Fabric Manager, but only those with a Web Tools license can be managed through Fabric Manager.

Fabric OS supports a maximum of five simultaneous HTTP sessions to any one switch. HTTP sessions are leveraged by every copy of Fabric Manager and Web Tools that are monitoring any one switch.

System Requirements

Fabric Manager V4.1 supports the following platforms:

- DS-8B and DS-16B series switches
- DS-16B2, and DS-32B2 series switches
- ED-12000B series switch
- Brocade Silkworm 2xxx, and 3xxx series switches
- Brocade Silkworm 12000 core switch
- Brocade Silkworm 6400

All references in this User Guide to the Connectrix B-Series and to Connectrix B-Series switches also apply to corresponding products from other suppliers of Brocade-based switch products.

You must enable HTTP on every switch that you want to discover, monitor, and configure with Fabric Manager.

For the following Fabric Manager features to run, you must enable HTTP on your SAN:

- Firmware download
- Sequenced reboot
- Port name change on switch
- License management
- Configuration handling
- Multifabric administration
- Topology/ISL monitoring

Some Fabric Manager features only run on particular firmware versions. Table 1-1 lists the features that only run on particular versions and the versions on which they run.

Table 1-1 Firmware-Specific Features

Feature	Firmware Version(s)
Port name change on a switch	3.1.0, 4.1.0, and higher
Topology/ISL monitoring	2.6.1, 3.1.0, 4.1.0, and higher

Table 1-1 Firmware-Specific Features (continued)

Feature	Firmware Version(s)
Security	2.6.1, 3.1.0, 4.1.0, and higher
Port swapping	4.1.0 and higher
FDMI/ HBA firmware download	3.1.0, 4.1.0, and higher

Fabric Manager Client

Fabric Manager client runs on the following operating systems:

- Windows 2000
- Windows NT 4.x
- Solaris 2.7 and 2.8

The Fabric Manager client needs to access the switches under management through an IP/Ethernet connection. It is not sufficient to only have access to the switches from the Fabric Managers server's machine in the case where the client and server are on different machines.

Web Tools requires a Java plug-in. Refer to your Release Notes .

Fabric Manager Server

Fabric Manager server runs on Windows 2000.

Each Fabric Manager server can support up to five Fabric Manager clients.

Advantages

Fabric Manager is the complete SAN management power tool for SANs and provides the following advantages to administrators:

- Provides a highly scalable Java-based application that manages multiple switches and multiple fabrics in real time.
- Assists SAN administrators with the configuration, monitoring, dynamic provisioning, and daily management of SANs.
- Lowers the cost of SAN ownership by intuitively facilitating SAN management tasks.
- Saves time by enabling the global integration and execution of processes across multiple fabrics through its single-point SAN management platform.
- Allows more effective management by providing rapid access to critical SAN information across both Fabric OS SANs and enhanced Fabric OS SANs.

Feature Highlights

Fabric Manager provides features to help you quickly and easily maintain, monitor, and configure your SANs.

Grouping

You can use Fabric Manager groups to:

- Simplify monitoring
- Simplify management
- Organize switches by function, switch type, firmware version, or any other criteria you choose
- Create functional hierarchies of groups

For more information, refer to Chapter 6, *Grouping*

ISL Monitoring

ISL checking monitors when you:

- Add a new ISL to the fabric
- Remove an ISL from the fabric
- Remove all ISLs between two switches in a fabric
- Plug an existing ISL into a different port on the same switch

For more information, refer to Chapter 13, *ISL Checking*.

Sequenced Reboot

With Fabric Manager you can define groups of switches to reboot simultaneously, and then configure groups to reboot sequentially. Reboot groups let you simultaneously reboot switches that run the same firmware, serve the same function, reside in the same physical location, or share any other attribute by which you want to group them.

For more information, refer to Chapter 18, *Sequenced Reboot*.

Firmware Download

Perform a firmware download with Fabric Manager to concurrently download firmware to multiple switches and (optionally) reboot the switches simultaneously or in sequence. For more information, refer to Chapter 12, *Firmware Download*.

License Management

Fabric Manager can display, store, load, and reload your license keys so that you do not lose them if your switch fails.

For more information, refer to Chapter 7, *Licensing*.

Fabric Merge Checking

Perform a fabric merge check to determine if you can merge two fabrics successfully. Fabric Manager provides the Fabric Merge Check feature to compare various configuration elements of two fabrics before you connect those fabrics. Fabric Manager extracts copies of configuration elements that can cause the fabric to segment and compares them in memory for inconsistency.

For more information, refer to Chapter 15, *Fabric Merge Check*.

Fabric Manager Server

The Fabric Manager Server is used for

- User authentication
- Data persistence
- Call home feature

Fabric Manager Terms and Concepts

Table 1-2 presents, alphabetically, Fabric Manager-specific terms and provides descriptions of each.

Table 1-2 Fabric Manager Terms and Concepts

Term	Description
Baseline	The configuration (from a file or on a switch) to which you compare other configurations, or that you download to one or more switches.
Direct connect remove	Event where you remove all ISLs between two switches.
Discovery	The process you perform to begin to monitor elements with Fabric Manager.
Export	Save content to a file to distribute settings to other users.
File log	File to which Fabric Manager stores log information. This log is not the log that appears when you click the **Open FM Log** icon.
Import	Open the contents of a file to add settings from other users.
Launch switch	The switch that uses the IP address that you type into the **Address** field when you discover a fabric. The name of the fabric matches the name of the launch switch unless you change the fabric name
Logical group	A collection of switches or ports that you designate to monitor or maintain as a unit.
Panel	A subwindow that appears in Detail view and Summary view
Stamp	A snapshot of the ISL topology of a fabric.
time out	Occurrence where a fabric does not stabilize within the amount of time that you configure during a sequenced reboot.
View	A Fabric Manager display.

2 Installing Fabric Manager

This chapter includes the following sections on installing Fabric Manager:

Introduction

This chapter describes how to install the Fabric Manager client and server software on the supported operating systems. Fabric Manager lets you choose from the following types of installation:

- Installing Fabric Manager Server
- Evaluation Version

Fabric Manager gives you the option of installing the following:

- Fabric Manager Server and Client
- Fabric Manager Client Only
- Fabric Manager Server Only

Installing Fabric Manager

You can choose to install a full version or an evaluation version of Fabric Manager V4.1.

Full Version

A valid serial number and license key are required for a full installation.

Evaluation Version

Fabric Manager offers an evaluation version for installation. The evaluation version lasts for 60 days. You do not need to provide a serial number or license key to use the evaluation version, however you must accept the agreement that is displayed during the installation.

Every time you launch Fabric Manager, a warning message notifies you when the evaluation installation will expire, and gives you the option to register Fabric Manager or continue with the evaluation version (see Figure 2-1).

Important Registering Fabric Manager requires the purchase of a license key and serial number from EMC (please allow up to 10 business days for delivery).

Figure 2-1 **Fabric Manager Evaluation Installation Version Warning**

After the 60th day, the evaluation version expires and an error message appears when you launch the trial version of Fabric Manager (see Figure 2-2).

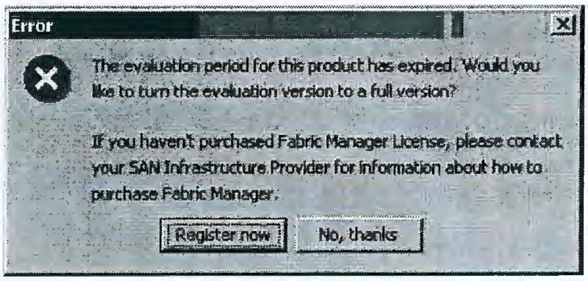


Figure 2-2 **Fabric Manager Evaluation Installation Version Expiration Error**

You can register the software to make it a full version or discontinue use of Fabric Manager.

Any time before the 60 days are up, you can convert your evaluation version to a full version by registering Fabric Manager. You can register Fabric Manager in any of the following ways:

- Click **Register Now** from the warning message that displays when you launch Fabric Manager every time during the 60-day evaluation period (see Figure 2-1)
- Click **Register Now** from the error message that displays when you launch Fabric Manager after the 60 day evaluation period is up (see Figure 2-2)

- Select **Register** from the **Help** menu in Fabric Manager. For detailed instructions, refer to *Registering Fabric Manager* on page 2-14.

Installing the Client and Server Together

To install the Fabric Manager server and client at the same time, perform the following steps:

1. Windows Environment: Double-click the **Windows** folder from the Fabric Manager Installation CD-ROM.

   Solaris Environment: Click **install.bin** from the File Manager window that appears when you insert the Fabric Manager Installation CD-ROM.

2. Double-click the **Install** icon. The **InstallAnywhere** dialog box runs, and then the **Fabric Manager** installation wizard appears (see Figure 2-3).

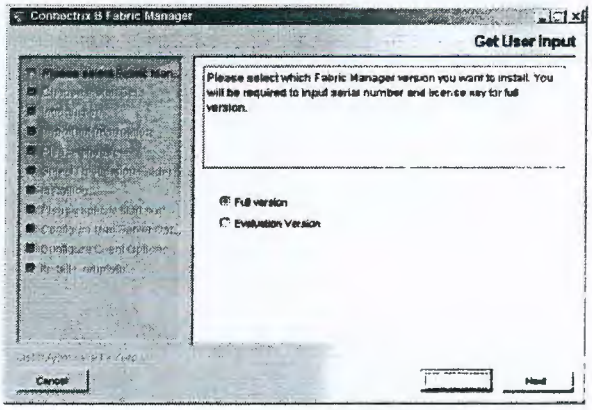


Figure 2-3 Fabric Manager Installation Wizard

3. Select the version you would like to install (evaluation or full), and click **Next**.
   The **User Input** screen appears.

   A valid serial number and license key are required for a full installation. You cannot continue the full installation process without a valid serial number and license key.

4. Enter a valid serial number and license key, and then click **Next**.

You will be prompted to wait while Fabric Manager configures your system. The **Choose Install Set** screen appears (see Figure 2-4).

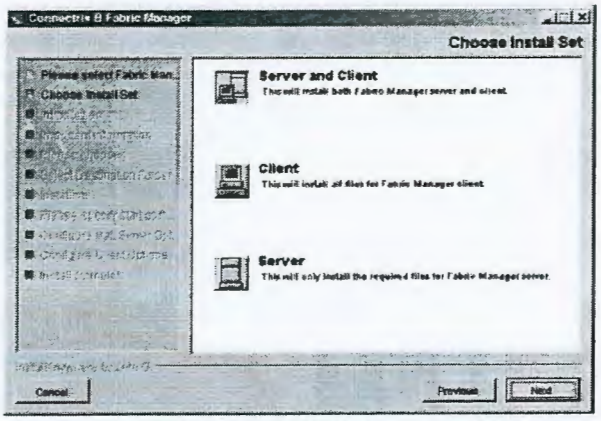


Figure 2-4 **Choose Install Set Screen**

5. Click the **Server and Client** icon, and click **Next**.

   The **Introduction** screen appears.

6. Read the **Introduction** and click **Next**.

   The **Important Information** screen appears.

7. Read the important information and click **Next**.

   The **Select Destination** (for Fabric Manager Client) screen appears (see Figure 2-5).

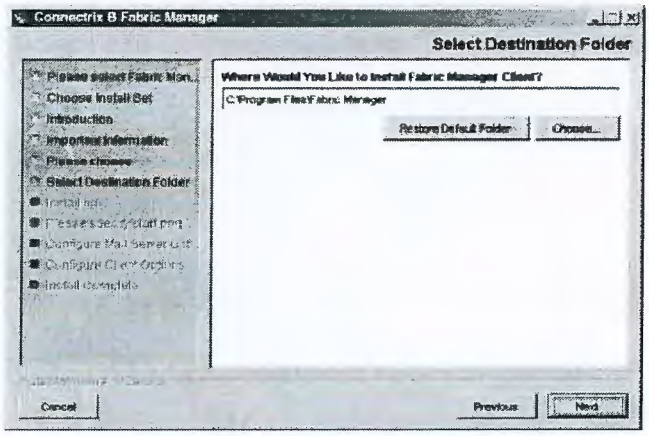


Figure 2-5 **Select Destination Folder for Fabric Manager Client**

Select a location to install the Fabric Manager client. The default location is

```
C:\Program Files\Fabric Manager
```

Click **Choose** to browse to another location.

Click **Next**. The **Select Destination Folder** (for Fabric Manager Server) screen appears (see Figure 2-6).

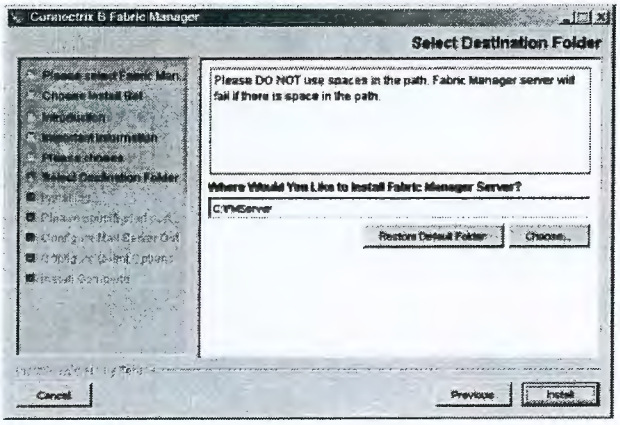


Figure 2-6 **Select Destination Folder for Fabric Manager Server**

8. Select a location to install the Fabric Manager Server. The default location is

   `C:\FMServer`

9. Click **Choose** to browse to another location.

   Do not include spaces in the directory path for the server.

   Click **Install**. You will be prompted to wait while Fabric Manager configures your system.

   The **Please Specify Starting Port Number** screen appears (see Figure 2-7).

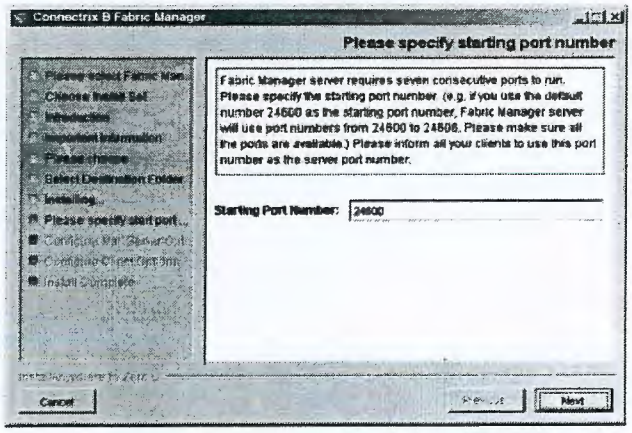


Figure 2-7 **Specify Starting Port Number for Fabric Manager Server**

10. Enter a starting port number.

    The port number you enter, and the next six ports, must be free ports. If you do not enter a free port number, the server will not start up correctly. Make note of the port number that you enter. When you install clients to access this server, you must use the same port number during the client installation.

    Click **Next**. You will be prompted to wait while Fabric Manager configures your system.

    The **Configure Mail Server Options** screen displays (see Figure 2-8).

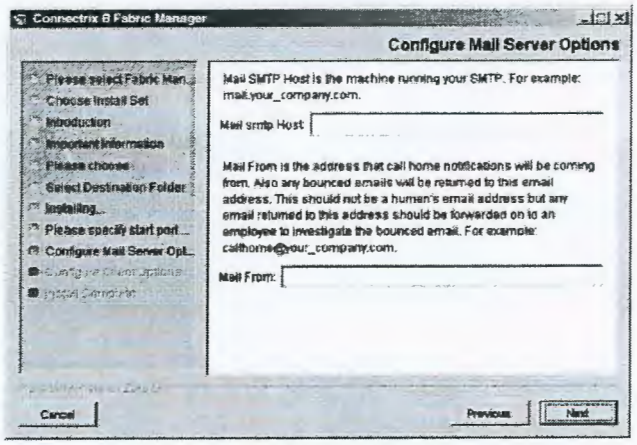


Figure 2-8 **Configure Mail Server Information**

11. In the **Mail SMTP Host** field, enter the SMTP/mail server to which the Fabric Manager server will send the Call Home e-mail notifications, and enter the e-mail address from which Call Home notifications will arrive in the **Mail From** field. Both are required.

    Click **Next**. The **Please Input Windows Domain Name** screen displays.

12. Enter your Windows domain name.

    Click **Next**. The **Important Information** screen appears.

13. Read the important information and click **Next**.

    The **Configure Client Options** screen appears (see Figure 2-9).

Figure 2-9 **Configure Client Options Screen**

14. Enter a Server IP address, and click **Next**.

    The **Install Complete Screen** appears.

15. Select **View Readme** if you would like to view the Readme file.

    Click **Done**.

Installing Fabric Manager Server

To install the Fabric Manager server, perform the following steps:

1. Windows Environment: Double-click the **Windows** folder from the Fabric Manager Installation CD-ROM.

   Solaris Environment: Click **install.bin** from the File Manager window that appears when you insert the Fabric Manager Installation CD-ROM.

2. Double-click the **Install** icon. The **InstallAnywhere** dialog box runs, and then the **Fabric Manager** installation wizard appears (see Figure 2-9).

3. Select the version you would like to install (evaluation or full), and click **Next**.

   A valid serial number and license key are required for a full installation. You cannot continue the full installation process without a valid serial number and license key.

4. Enter a valid serial number and license key, then click **Next**. You will be prompted to wait while Fabric Manager configures your system. The **Choose Install Set** screen appears (see Figure 2-4 on page 2-5).
5. Click the **Server** icon, and click **Next**. The **Introduction** screen appears.
6. Read the introduction information, and then click **Next**. The **Select Destination Folder** screen appears.
7. Select a location to install the Fabric Manager Server. The default location is

   ```
   C:\FMServer
   ```

   Click **Choose** to browse to another location.

   Do not include spaces in the directory path for the server.

   ---

8. Enter a starting port number.

   The port number you enter, and the next six ports, must be free ports. If you do not enter a free port number, the server will not start up correctly. Make note of the port number that you enter. When you install clients to access this server, you must use the same port number during the client installation.

   Click **Next**. You will be prompted to wait while Fabric Manager configures your system.

   The **Configure Mail Server Options** screen appears (see Figure 2-8 on page 2-8).
9. In the **Mail SMTP Host** field, enter the SMTP/mail server to which the Fabric Manager server will send the Call Home e-mail notifications. In the **Mail From** field, enter the e-mail address from which Call Home notifications will arrive. Both are required.

   Click **Next**. The **Please Input Windows Domain Name** screen displays.
10. Enter your Windows domain name. Click **Next**. The **Important Information** screen appears.
11. Read the important information and click **Next**. The **Install Complete** screen appears.

12. Select the **View Readme** checkbox if you would like to see the Readme file.
    Click **Done**.

Installing Fabric Manager Client

To install the Fabric Manager client, perform the following steps:

1. Windows Environment: Double-click the **Windows** folder from the Fabric Manager Installation CD-ROM.

   Solaris Environment: Click **install.bin** from the File Manager window that displays when you insert the Fabric Manager Installation CD-ROM.

2. Double-click the **Install** icon. The **InstallAnywhere** dialog box runs, and then the **Fabric Manager** installation wizard appears (see Figure 2-3 on page 2-4).

3. Select the version you would like to install (evaluation or full), and click **Next**.
   The **Introduction** screen appears.

   A valid serial number and license key are required for a full installation. You cannot continue the full installation process without a valid serial number and license key.

4. Click the **Client** icon, and click **Next**.
   The **Introduction** screen appears.

5. Read the introduction and click **Next**.
   The **Important Information** screen appears.

6. Read the important information and click **Next**.
   The **Select Destination Folder** screen appears.

7. Select a location to install the Fabric Manager Client. The default location is

   ```
   C:\Program Files\Fabric Manager
   ```

   Click **Choose** to browse to another location.

   Click **Next**. The **Configure Client Options** screen appears (see Figure 2-10).

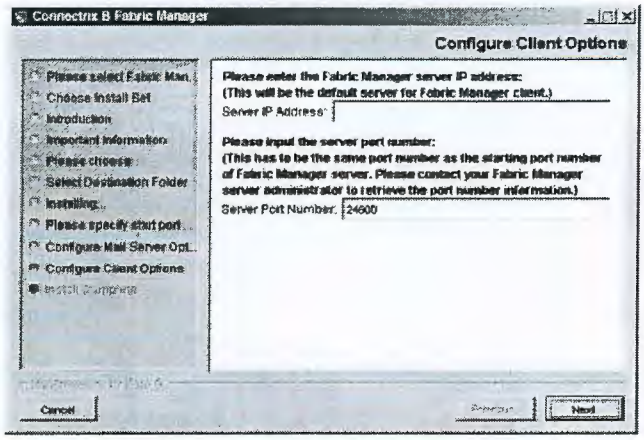


Figure 2-10 Configure Client Options Screen

8. Enter a **Server IP Address** and a **Server Port Number**.

   The **server IP address** you enter will be the default server for the Fabric Manager client.
   The **server port number** *must* be the same port number as the starting port number of the Fabric Manager server.

   Click **Next**. The **Install Complete** screen appears.

9. Select the **View Readme** checkbox if you would like to see the Readme file.
   Select the **Launch Fabric Manager** checkbox if you would like to launch Fabric Manager.
   Click **Done**.

   For Solaris operating systems only: Log out of your workstation and log in again to access all Fabric Manager features.

Launching Fabric Manager for the First Time

To launch Fabric Manager, perform the following steps:

1. From the **Start** menu, select **Programs, Fabric Manager, Fabric Manager**. The **Fabric Manager Login** dialog box appears. Fabric Manager automatically populates the **Server** and **Port** fields of the dialog box with the values that you specified when you installed the application. Figure 2-11 shows the user login dialog box.

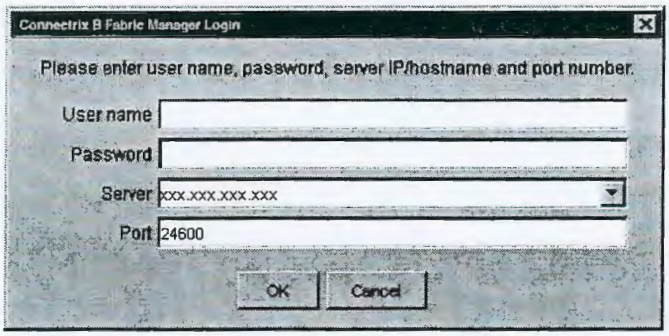


Figure 2-11 Fabric Manager Login Dialog Box

2. In the **User name** field, enter the username that you use to log in to the server.

   Fabric Manager will store your username and automatically populate this field when you subsequently launch the software. *No user names may contain the following characters that appear in bold text:* **\/:*?"<>|** *as per Windows limitations.*

3. In the **Password** field, enter the password that you use to log in to the server and click **OK**. Fabric Manager launches.

   Usernames and passwords correspond to Windows domain usernames and passwords.

Registering Fabric Manager

During a full installation, Fabric Manager is automatically registered if you responded to the prompt with a valid license key and serial number. If you install the evaluation version of Fabric Manager, you need to register Fabric Manager within 60 days of installing. After 60 days, the evaluation version will not be usable until it is registered, which changes it into a full version.

Important Before you can register Fabric Manager, you must purchase a license key and serial number from EMC (please allow up to 10 business days for delivery).

To register Fabric Manager, perform the following steps:

1. Select **Register** from the **Help** menu.
   The **Fabric Manager Registration** window appears.
2. Enter a valid serial number and license key.
3. Click **Register**. A **Congratulations** dialog box appears, indicating that you have successfully registered Fabric Manager.
4. Click **OK** in the **Congratulations** dialog box.
5. Click **Cancel** to close the **Fabric Manager Registration** window.

Uninstalling Fabric Manager

Windows Operating Systems

1. From the **Start** menu, select **Programs, Fabric Manager , Uninstall Fabric Manager.**
2. Click **Next**.
3. Click the **Complete Uninstall** icon to remove both the Fabric Manager client and server from your machine, or click the **Uninstall Specific Features** icon and proceed as follows:
   a. Click **Next**.
   b. Clear the checkboxes of the features that you want to uninstall.
   c. Click **Uninstall**.
4. Click **Done**.

Solaris Operating Systems

1. From the **UninstallerData** directory, run **Uninstall_FabricManager**.
2. Click **Next**.
3. Click the **Complete Uninstall** icon and click **Next**.
4. Click **Done**.

3 Fabric Manager Interface

This chapter includes the following sections:

Introduction

The basic Fabric Manager graphical user interface (GUI) uses icons, menus, and right-click menus to help you administer your SANs more quickly and easily. This chapter identifies many of the visual elements that you see when you open Fabric Manager. This chapter focuses on icons that appear in Summary view. Specific chapters and appendices in this user guide address icons and menus that appear in other views.

For more detailed information on Summary view, refer to Appendix C, *View Menu Reference*, *Summary View* on page C-14.

Basic GUI

The basic Fabric Manager GUI includes standard menus, tabs, and pull-down menus as well as custom icons and windows. Figure 3-1 shows the basic Fabric Manager interface.

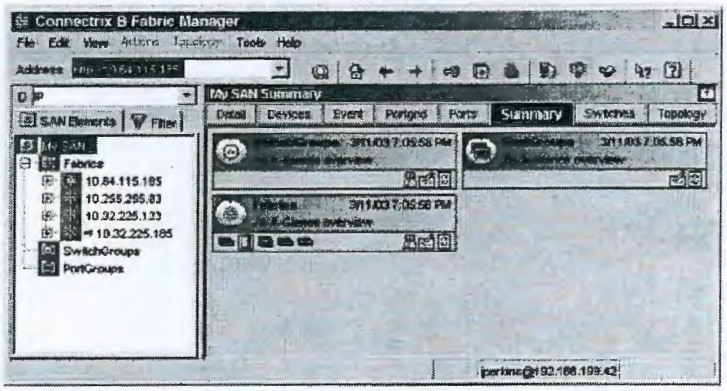


Figure 3-1 **Fabric Manager GUI in Summary View**

For information on the menus that appear in the interface, refer to the appropriate appendix. This user's guide explains each menu and all nested elements in separate appendices.

This chapter describes the following GUI elements:

- **Address** field
- Icons and panels
- **ID** pull-down menu
- **SAN Elements** tab
- **Filter** tab

Address Field

Use the **Address** field to discover a new fabric. The **Address** field keeps a pull-down-menu list of the fabrics that you have discovered and lets you enter the IP address of new switches and fabrics that you want to monitor.

Standard Fabric Manager Icons and Panels

Standard icons appear in the Fabric Manager display, and different panels appear in the display when you use Summary view or Detail view. Table 3-1 lists and describes standard Fabric Manager icons. Additional icons appear in certain views; you can find descriptions of those icons in the appropriate View Menu appendix.

Table 3-1 Standard Icons

Icon	Description
Subnet scan icon ( )	Opens the **Subnet scan** dialog box to help you discover fabrics. For more information, refer to *Run a Subnet Scan* on page 4-2.
Home icon ( )	Returns to the view that appeared when you opened Fabric Manager.
Previous icon ( )	Returns to the previous view in the navigation history (if applicable). If you click the **Previous** icon for more than half a second, a menu showing the previous ten views appears. You can select one of the views or select cancel.
Next icon ( )	Moves forward to the next view in the navigation history (if applicable). If you click the **Next** icon for more than half a second, a menu showing the previous ten views appears. You can select one of the views or select cancel.

Table 3-1 Standard Icons (continued)

Icon	Description
Fabric login icon ( )	Opens the **Fabric login** window so you can log in to one or more switches. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
Open FM Log icon ( )	Opens the Fabric Manager log for support purposes.
Print View icon ( )	Prints the contents of the view. You cannot access this option in all views. You can click this icon when you open any of the following views: ◆ Devices ◆ Event ◆ Port grid ◆ Ports ◆ Switches ◆ Topology You cannot click this icon when you open any of the following views: ◆ Detail ◆ Summary
Firmware download to HBAs icon ( )	Opens the **Firmware download to HBAs** window. For more information, refer to *Download Firmware to an HBA* on page 19-2.
Firmware download to switches icon ( )	Opens the **Firmware download to switches** window. For more information, refer to Chapter 12, *Firmware Download*.
Sequenced reboot icon ( )	Opens the **Sequenced reboot** window. For more information, refer to Chapter 18, *Sequenced Reboot*.
Context Help icon ( )	Changes your pointer to the help pointer. Click an element of the GUI for context-sensitive help.
Help icon ( )	Opens Fabric Manager Help.

Panels appear in Summary view and Detail view to display information about elements in the **SAN Elements** tab. Figure 3-2 displays a panel in Summary view.

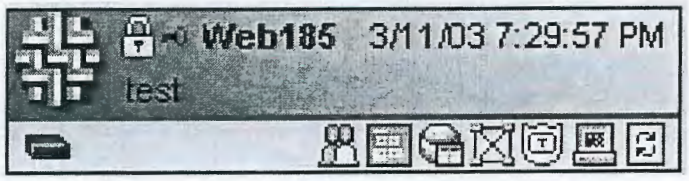


Figure 3-2 Example Fabric Manager Panel

Panels contain content and icons that you can use to monitor and configure your SAN. For more information, refer to *Detail View* on page C-2 and *Summary View* on page C-14.

ID Field

The **ID** pull-down menu lets you customize how you view your switches and fabrics. For instructions on how to select identities with the ID field, refer to *Select Identity* on page 4-9.

SAN Elements Tab

The **SAN Elements** tab displays the various elements that you monitor with Fabric Manager. As you use Fabric Manager, you repeatedly select items from the **SAN Elements** tab that you then configure and monitor.

When an element that Fabric Manager monitors changes status, the element changes color in the **SAN Elements** tab. Furthermore, the parent items in the **SAN Elements** tab tree change color to match.

Port status does not affect the switch status color.

When an item in your **SAN Elements** tab changes color, the change does not necessarily represent the failure of an entire fabric or switch. Expand the navigation tree to identify the source of the status change.

Filter Tab

The filter tab lets you view elements that include a particular alphanumeric string. For instance, if you name all switches for your Accounting team acct*X*, where *X* is a number, you can view just your accounting switches if you select **name** from the pull-down menu, type **`acct`** in the text field, and click **Enter**. The **Filter** tab displays every switch that has `acct` in its name.

You can filter elements by the following attributes:

- IP
- Name
- Switch Type
- Version
- WWN
- Domain ID

4 Common Fabric Manager Tasks

This chapter contains the following sections:

Introduction

This chapter explains how to perform common Fabric Manager tasks. More complicated or mission-critical tasks appear in separate chapters later in this user's guide.

Discover a Fabric

You must *discover* a fabric to add it to the **SAN Elements** tab and administer it with Fabric Manager. To discover a fabric, perform the following steps:

1. Place your cursor in the **Address** field and delete the contents of the field.
2. In the **Address** field, enter the IP address or switch name of a switch in the fabric that you want to administer and press ENTER.

   You do not need to include `http://` before the IP address to discover a fabric.

Run a Subnet Scan

Switches may appear in your subnet scan even after you unplug the Ethernet cables of those switches.

1. From the **Tools** menu, select **Subnet scan...** The **Subnet scan** dialog box opens.
2. Enter the first three sets of digits of an IP address in the first three sections of the **IP Address Range** field.

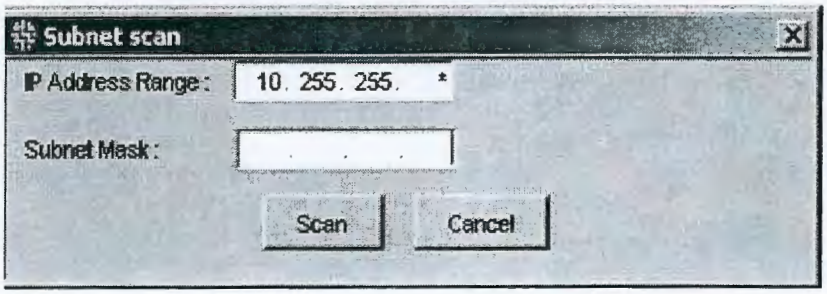


Figure 4-1 Example IP Address Range

3. Enter a wildcard in the last section of the **IP Address Range** field to represent the range of scan. Choose from one of the following three options:

- **192.168.168.*** discovers any fabric in the address range of 192.168.168.0–192.168.168.255.
- **192.168.168.1**** discovers any fabric in the address range of 192.168.168.100–192.168.168.199. (The first digit in the wildcard cannot exceed a value of two; see note.)
- **192.168.168.11*** discovers any fabric in the address range of 192.168.168.110–192.168.168.119. (See note.)

The number before the "*"can be any number so long as the resulting range is between 0 and 255. For example, you cannot enter 192.168.168.3** or 192.168.168.26*. Also, if you enter 192.168.168.25*, the range will be 192.168.168.250–192.168.168.255.

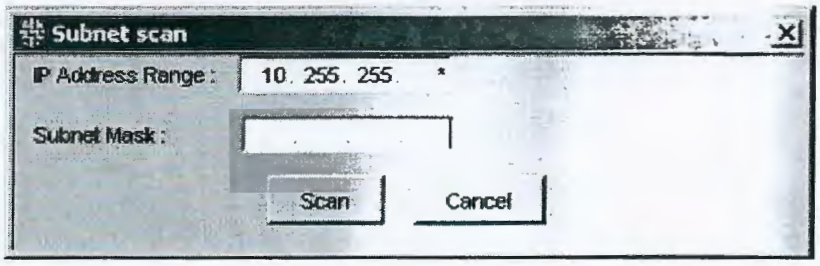


Figure 4-2 Example IP Address Range

4. Enter a subnet mask to avoid scanning the IP address for the network or broadcasting.

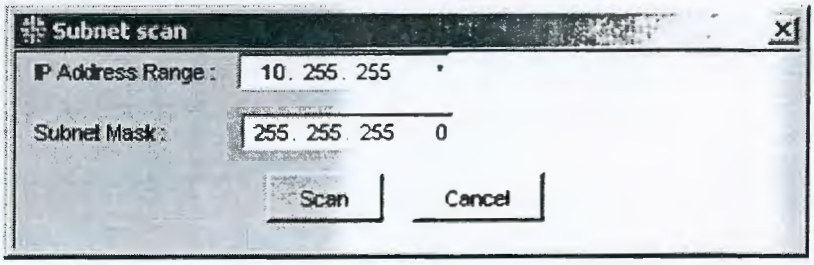


Figure 4-3 Example Subnet Mask

5. Click **Scan**. The scan result appears. IP addresses that appear as underlined links with two angle brackets (>>) represent fabrics. Click the link to view the switches in the fabric.

To add a switch or fabric to your **SAN Elements** tab, click the checkbox next to the element, and then click the **Add** button.

Delete a Fabric

1. In the **SAN Elements** tab, click the fabric that you want to remove from Fabric Manager.
2. Press DELETE to remove the fabric. Fabric Manager will prompt you to make sure that you want to delete the fabric.

You can also select **Delete** from the **Actions** menu to remove the selected fabric from Fabric Manager.

Switches and ports from this fabric that you added to logical switchgroups and portgroups still appear in the groups.

Manually Refresh a Fabric

All At-a-Glance Views are updated at 20-second intervals; everything else in the GUI is updated whenever there is a change in current data. If you notice a discrepancy between the data displayed in Fabric Manager and the fabric itself, perform a manual refresh (or *rediscover*) the fabric to update the GUI.

1. In the **SAN Elements** tab, click the fabric that you want to refresh.
2. From the **Actions** menu, select **Refresh**.

This action disables ISL Checking and Fabric Checking on your fabric. You must reenable the features once the refresh is complete.

Rename a Fabric

1. In the **SAN Elements** tab, click the fabric that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor appears to the right of the current name.

   You can also use the F2 key, or click and expand a fabric, switch, or port icon three times to rename it.
3. Rename the fabric and press ENTER.

Rename a Switch

1. In the **SAN Elements** tab, click the switch that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor appears next to the name of the switch in the **SAN Elements** tab.
3. Edit the name of the switch and press ENTER.

You can also use the F2 key, or click and expand a fabric, switch, or port icon three times to rename it.

Rename a Port

1. In the **SAN Elements** tab, click the port that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor appears next to the name of the switch in the **SAN Elements** tab.
3. Edit the name of the port and press ENTER.

You can also use the F2 key, or click and expand a fabric, switch, or port icon three times to rename it.

View SAN Information

Table 4-1 Fabric Manager Views

View	Description
Detail	Provides information about the components and status of an element.
Devices	Provides information about all devices that connect to an element.
Event	Provides an event log for the element and the status reason.
Portgrid	Displays the node that connects to each port. The Portgrid view displays devices only; it does not show ISL information.
Ports	Provides information about the status and traits of each port.
Summary	Provides a summarized version of Detail view. Summary view provides the same view options as Detail view. Customize Summary view to display content that you frequently reference. Customize Detail view to provide a more thorough report. For more information, refer to *Customize a View* on page 4-7.
Switches	Provides information about the status and traits of each switch.
Topology	Provides a graphical display of topology.

Customize a View

1. Click an element in the **SAN Elements** tab.
2. From the **View** menu, select the view that you want to customize.
3. From the **Edit** menu, select **View Options...** The **Edit View Options** window appears.
4. Click an item, and then click the appropriate directional arrow to add items to the display or remove items from the display. You can use the Ctrl and Shift keys to select multiple items at once. In the view display columns, designate the order of the columns as follows:
   a. Click an item in the **Display Items** field.
   b. Click an up or down directional arrow to change the order of the column in the display.
5. Click **OK**.

Change Panel Descriptions

1. In the **SAN Elements** tab, click the element that you want to change.
2. From the **Edit** menu, select **Change Description**. The **Please enter the new description** dialog box appears.
3. In the **New Description** field, enter a description for the panel and click **OK**. To view the description, click the parent element in the **SAN Elements** tab. The new description appears on the appropriate panel.

Log In To Multiple Switches Simultaneously

- Firmware download to HBAs and switches
- License key installation
- Fabric compare and merge
- Date/time synchronization
- Baseline configuration upload/download
- Sequenced reboot
- Security policy configuration
- Fabric backup
- Diff with backup

1. From the **File** menu, select **Fabric Login...**
2. Select switches or fabrics from the **SAN Elements** tab and click the right arrow to move them to the **Selected Switches** window.

   Click and drag fabrics or switches to quickly move switches into the **Selected Switches** window.

3. In the **User Id** field, enter your user ID.
4. In the **Password** field, enter your password.
5. Click **Apply**. The success or failure of the login appears in the **Status** column of the **Selected Switches** window. A key icon (🔑) appears next to each switch and fabric that completes a successful login.

If you did not log in to all of the switches successfully, remove the successful switches from the **Selected Switches** window and retry with a new user ID and password.

Select Identity

From the **ID** pull-down menu, select the type of identifier that you want to use to label the elements in your display.

Navigate Fabric Manager

Navigate with Elements and Views

From the **View** menu, select the view that you want to access:

1. Use the view selector. To use the view selector, perform the following steps:
   a. Click the **Display view selector** icon ( ) in the top-right corner of the interface. The view selector appears.

Figure 4-4 View Selector

   b. In the view selector, click the view that you want to access.

The icon that displays the view selector ( ) serves other functions when it appears in other locations. Only the icon in the top-right corner of the interface will display the view selector.

Table 4-2 Fabric Manager Views

View	Description
Detail	Provides information about the components and status of an element.
Devices	Provides information about all devices that connect to an element.
Event	Provides an event log for the element and the status reason.

Table 4-2 Fabric Manager Views (continued)

View	Description
Portgrid	Displays the node that connects to each port. The Portgrid view displays devices only; it does not show ISL information.
Ports	Provides information about the status and traits of each port.
Summary	Provides a summarized version of Detail view. Summary view provides the same view options as Detail view. Customize Summary view to display content that you regularly reference. Customize Detail view to provide a more thorough report. For more information, refer to *Customize a View* on page 4-7.
Switches	Provides information about the status and traits of each switch.
Topology	Provides a graphical display of topology.

Navigate with Navigation Buttons and History

- Click the **Back** button ( ) to return to the previous view.
- Click and hold the **Back** button to display a list of the views that you have visited; then drag the mouse to the view you want to see and release the mouse button.
- Click the **Forward** button ( ) to move forward to the next view in your view history.
- Click and hold the **Forward** button to display a list of the views that you have visited; then drag the mouse to the view you want to see and release the mouse button.
- Click the **Home** button ( ) to display the view that appeared when you launched Fabric Manager.

Customize Tables

- Click and drag table headers to change the order in which columns appear in the table.
- Click and drag the border between column headers to resize columns.
- Click column headers to organize information in ascending or descending order by that column.

The **Status** column in Portgrid view and Switches view sorts contents by severity when you click the column header.

Copy Tables to Spreadsheet Applications

1. Navigate to a view that displays a table.
2. From the **Edit** menu, select **Copy Table**.
3. Open a spreadsheet application.
4. From the **Edit** menu, select **Paste**.

Enable/Disable Elements

1. Verify that you have logged in to all necessary switches. You cannot enable or disable a port or switch until you log in to that switch. For more information on how to log in, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. From the **SAN Elements** tab, select the switches, ports, or groups that you want to disable.
3. From the **Actions** menu, select **Disable/Enable...** and click the appropriate option.

The switch enable/disable menu item enabling/disabling is based on switch status; that is, when the switch is disabled, only the switch-enable menu item is enabled, the switch disable menu item is greyed out, and vice versa. For Telnet, switch enable/disable commands can be executed regardless of switch status.

Configure Log Parameters

CAUTION

Do not change log parameters unless support personnel instruct you to do so.

1. From the **File** menu, select **Options...** The **Options** window opens.
2. From the **Configurations** navigation tree, click **Log Parameters**.
3. In the **Log Directory Path** field, enter a directory or click **Browse** to select a directory to store the log directory.
4. From the **FabricManager Log Level** pull-down menu, select a severity level. Fabric Manager will log all events of that severity level and lower.
5. From the **File Log Level** pull-down menu, select a severity level. Fabric Manager will log all events of that severity level and lower.
6. Click **OK**.

Print

- Devices
- Event
- Portgrid
- Ports
- Switches
- Topology

1. From the **View** menu, select a view that Fabric Manager can print.
2. From the **File** menu, select **Print...** The **Print** dialog box opens.
3. Select a printer and click **OK**.

Print in One Page

The option to print in one page applies exclusively to Topology view.

1. From the **View** menu, select a view that Fabric Manager can print.
2. From the **File** menu, select **Print In One Page...** The **Print** dialog box opens.
3. Select a printer and click **OK**.

Download a Configuration

Download to Switches from a Baseline File

1. From the **Tools** menu, select **Config, Compare/Download from File**. The **Compare/Download from File—Select Baseline Configuration** dialog box opens.
2. Navigate to the baseline file and click **Open**. The **Compare/Download from File—Target Switch Selection** window opens.
3. From the **SAN Elements** tab, select switches you want to compare and move them to the right-hand window and click **OK**. You can:
   - Navigate to a switch, click the switch, and then click the right arrow.
   - Click and drag a switch from the **SAN Elements** tab to the right-hand window.
   - Press and hold CTRL, click multiple switches in the **SAN Elements** tab, and click the right arrow.
   - Press and hold CTRL, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the right-hand window.
   - Click and drag a fabric to the right-hand window to move. Add all of the switches in that fabric to the window.

   The **Compare/Download from File—Switch Configuration comparison and Download** window opens.
4. Click **Apply Baseline...**

The delay timer at the bottom of the **Apply Baseline...** dialog box cannot be configured from this dialog box. It is propagated from current settings in the sequenced reboot group and represented by the combination of "Fabric Stabilization timeout" and "Delay after Fabric Stabilization" parameters.

Prompts will appear to ensure that you do not download a configuration accidentally.

The **Apply Baseline** window opens. The **root** navigation tree divides the switches into the following two groups:

- Non-Reboot Config Group: These switches are Linux-based and do not need to reboot after a config download.
- Reboot Config Group: These switches are VXWorks-based and must reboot after a config download.

5. Click **Apply**. Fabric Manager will prompt you to be sure that you want to proceed. The download proceeds one group at a time. The status of the switches appears in the right-hand window.

Download to Switches from a Baseline Switch

1. From the **Tools** menu, select **Config, Compare/Download from Switch**. The **Compare/Download from Switch–Source Configuration Selection** window opens.
2. Navigate to the switch that you want to use as a baseline and click the right-pointing arrow to move that switch to the right-hand window.
3. Click **OK**. The **Compare/Download from Switch–Target Switch Selection** window opens.
4. From the **SAN Elements** tab, select switches you want to compare and move them to the right-hand window. You can:
   - Navigate to a switch, click the switch, and then click the right arrow.
   - Click and drag a switch from the **SAN Elements** tab to the right-hand window.
   - Press and hold CTRL, click multiple switches in the **SAN Elements** tab, and click the right arrow.
   - Press and hold CTRL, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the right-hand window.
   - Click and drag a fabric to the right-hand window to move add all of the switches in that fabric to the window.
5. Click **Apply Baseline...**

6. From the **Select Protocol** pull-down menu, select **File Transfer Protocol(ftp)**.
7. In the **Password Required for FTP** field, enter your password and click **OK**.
8. Click **Test** to ensure that you can access the FTP server specified. Fabric Manager will report success or failure.

In addition to validating connectivity to the FTP server, the Test button writes a temporary file to the FTP server. Write permissions must be set up properly on the specified path of the FTP server for the test to complete successfully.

---

9. Click **OK** to save settings.

Configure File Transfer Options

1. From the **File** menu, select **Options...** The **Options** window opens, as shown in Figure 4-5.

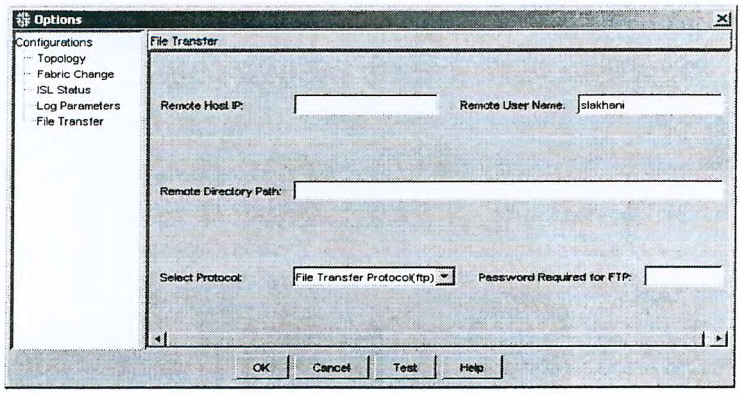


Figure 4-5 **Options Window**

2. The default view in the **Options** window is the File Transfer view. If the File Transfer view is not displayed, select **File Transfer** from the **Configurations** navigation tree (Figure 4-6).

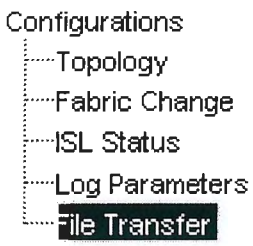


Figure 4-6 **Options Window Configurations Tree**

3. In the **Remote Host IP** field, enter the IP address of your FTP server.
4. In the **Remote User Name** field, enter your login name.
5. In the **Remote Directory Path** field, enter a default FTP directory.

   Do not enter a file name, only a directory.

Synchronize Time and Date across a Fabric

To synchronize time and date, you must choose fabrics, not switch groups.

1. Log in to the switches in the fabric that you want to synchronize. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. In the **SAN Elements** tab, click the fabric that you want to synchronize.
3. From the **Action** menu, select **Set Time...** The **Time** dialog box opens (Figure 4-1.)

Figure 4-7 **Time Dialog Box**

4. To adjust the time or date, click the appropriate field in the **Time** dialog box and use the up and down arrows to iterate the value; then click **OK**.

Filter Elements

The Filter tab consists of the following three components:

- A text field
- A pull-down menu
- A **SAN Elements** field

To use the Filter tab:

1. From the pull-down menu, select an identifier. For more information, refer to *Filter Tab* on page 3-6.
2. In the text field, type text (letters, numbers, or symbols such as a period) that appears in the elements that you want to view. For example, to view elements that all include **`switch`** in the name, select **Name** from the pull-down menu and enter **switch** in the text field. To view elements that include **10.32** in the IP address, select **IP** from the pull-down menu and enter **`10.32`** in the text field.
3. Press ENTER. Every element that includes the text that you entered appears in the **SAN Elements** field.

Designate a Switch as a Core Switch

This procedure applies only to Core Edge topologies.

1. From the **SAN Elements** tab, click the switch that you want to designate.
2. From the **Actions** menu, select **Core Switch**. When you view the fabric that switch belongs to in Topology view and select the core-edge layout, your switch will appear as a core switch.

5 User Logins and Persistence

This chapter includes the following sections:

Introduction

Fabric Manager 4.0 requires that the user log in to use the software, and it stores user-specific settings for each user. Figure 5-1 shows the login dialog box.

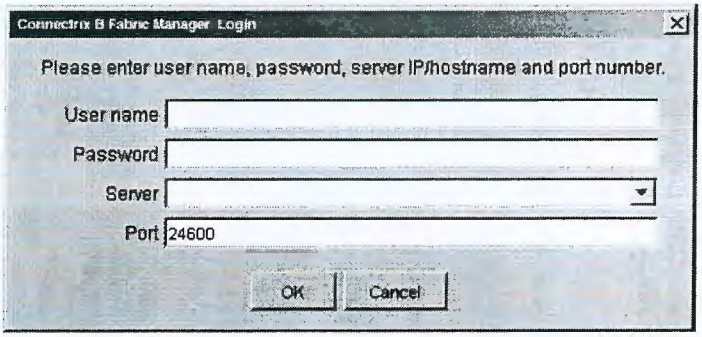


Figure 5-1 **Fabric Manager Login Dialog Box**

Fabric Manager stores user settings when you exit, *not while you run the software.* Some persistent settings reside on the server and others reside on the client. If the client cannot access the server at exit, Fabric Manager alerts you that your settings will not persist.

When the client attempts to log in to the server, the server authenticates the client login. After the server authenticates the client, Fabric Manager launches and polls switches.

Log-In Scenarios

After you log in to Fabric Manager, connection problems may arise that can potentially interfere with the client. The following two scenarios occur most commonly:

1. While your client runs, your password changes on the server. When you try to close the client and store your settings, the client prompts you to enter your password. You must enter the new password to persist your data and close the client.
2. While your client runs, the server goes down. When you try to close the client, the client alerts you that you cannot persist your settings. The client gives you the option to close and lose your settings or wait until the server comes back up. When the server comes back up, you can exit and your settings persist.

Data That Persists

Fabric Manager stores the following user settings:

Locally

- Username
- Host name/server IP address of all servers you have successfully accessed
- Port numbers
- Browser path to launch Web Tools
- Dimensions of the Fabric Manager window
- Fabric Manager log directory path

Remotely

- Group definitions
- Discovered fabrics
- UI settings (view customizations, topology locations, and so on)
- Switch usernames and passwords

Persistence Files

Prior to Fabric Manager V4.0, two files stored user information locally. Table 5-1 lists and describes those files.

Table 5-1 Original Fabric Manager Persistence Files

File	Contents
`FabricManager.properties`	UI settings and configurable parameters
`FabricManager.xml`	Discovered fabrics and group definitions

To adapt to the client-server architecture of Fabric Manager V4.0, some of the content of the `FabricManager.properties` file now appears in a `FabricManagerUser.properties` file that resides on the server. Table 5-2 lists and describes the files that store user settings.

Table 5-2 Current Fabric Manager Persistence Files

File	Location	Contents
`FabricManager.properties`	client	Fabric Manager server usernames and port
`FabricManager.xml`	server	Discovered fabrics and group definitions
`LocationTable`	server	X and Y locations for topology nodes in Topology view
`FabricManagerUser.properties`	server	User interface settings such as window dimensions, known fabrics, file transfer settings, and default layout and link styles for the Topology view
`SwitchInfo.txt`	server	Login information with passwords encrypted

6 Grouping

This chapter includes the following sections:

Introduction

Logical *groups* consist of SAN elements (either switches or ports) that you select to monitor as a unit. When you click a group in the **SAN Elements** tab and select Summary view, you immediately see the status of the switches or ports that you added to the group. You can use groups to:

- Simplify monitoring
- Simplify management
- Organize switches by function, switch type, firmware version, or any other criteria that you choose
- Create functional hierarchies of groups

Create groups of similar switches and ports so you can monitor and configure them as a unit instead of individually. For instance, if you create a group of switches that run the same firmware, you can download new firmware to those switches as a group rather than one by one. Whenever you need to perform the same task on multiple switches, you can save time if you create a group and perform that task on the group. Examples of such tasks include:

- Multiple switch login
- Simultaneous firmware downloads
- Fabric-wide license key activations

A switch can appear in multiple groups at the same time.

Groups persist on your server in your `FabricManager.xml` file. You can import and export groups so that multiple users can share group definitions.

Switches remain in a group even if you remove their source fabrics from Fabric Manager. That is, if switch X is in fabric Y and you add it to group Z, switch X remains in group Z even after you delete fabric Y from Fabric Manager.

Furthermore, when you look at a logical switch group in the Topology view, links will disappear if the switches that are in this group are no longer in the SAN Elements tab in Fabric Manager.

Best Practices

The following list describes valuable ways to use Fabric Manager groups:

- Create groups of switch model types or firmware versions to expedite firmware downloads.
- Group switches by function to monitor switches that belong to different departments or that serve as a backbone to the SAN.
- Group switches by physical location to monitor fabrics in disparate locations.
- Group switches by SAN island to monitor or update individual islands.
- Group switches by redundancy so you can maintain half of a fabric while the other half continues to carry traffic.
- Nest fabrics to drill down to the source of a problem. For instance, if you create a switch group for a campus and then nest within that switch group for departments, you can move down the hierarchy to determine the source of any status change.
- Create separate groups for monitoring and management to reduce unnecessary levels of nesting.
- Group ports by certain devices and hosts to more easily monitor those elements.
- Use groups to simplify the monitoring view of a large or complex fabric.

When you remove a switch from a fabric, you must remove that switch from all group definitions because Fabric Manager does not do so dynamically. For the same reason, if you replace the switch with a new switch, you must add that switch to all applicable group definitions.

Create a Group

With Fabric Manager, you can create a group of switches or a group of ports. Group switches together that serve similar purposes (for instance, all core switches or all switches that run the same firmware) and group ports together that serve similar purposes (for instance, all E_Ports).

Create SwitchGroups

A switch group consists of a collection of switch identifiers. After you create a group, you can click and drag that group during tasks to work with all switches at once. For instance, if you want to log in to all of the switches in a group, you can drag the group into the appropriate window so you do not need to select each individual switch. To create a group of switches, perform the following steps:

1. From the **File** menu, select **Groups, Edit Switch Groups...** The **Edit Switch Groups** dialog box appears.
2. Click the **SwitchGroups** icon in the right-hand window.

   The group that you create appears nested within the item that you click in this step. If you click an existing group instead of the **SwitchGroups** icon, your new group will appear as a subgroup of that group. After you create a group, you can click and drag it to a new location in the hierarchy.

3. Click **Create...** The **Create Group** dialog box appears.
4. Type a name for your group in the **Name** field and click **OK**.
5. Click the icon of the group that you created.
6. In the left-hand window, click the switch that you want to add to your group, and then click the right arrow to add the switch to the group.

   To add multiple switches at once, press and hold CTRL as you click additional switches, or simply click and drag any node in the tree to add the switches from that node.

   Click and drag switches directly from the left-hand window to the switch group to more quickly populate the group.

7. Click **OK** after you add switches to your group. The group appears in the **SAN Elements** tab under **SwitchGroups**. To view the contents of the group, click the group.

Create PortGroups

A port group essentially consists of a collection of port identifiers. After you create a group, you can click and drag that group during tasks to work with all ports at once. Perform the following steps to create a group of ports:

1. From the **File** menu, select **Groups, Edit Port Groups...** The **Edit Port Groups** dialog box appears.
2. Click the **PortGroups** icon in the right-hand window.

   The group that you create appears nested within the item that you click in this step. If you click an existing group instead of the **PortGroups** icon, your new group will appear as a subgroup of that group. After you create a group, you can click and drag it to a new location in the hierarchy.

3. Click **Create...** The **Create Group** dialog box appears.
4. Type a name for your group in the **Name** field and click **OK.**
5. Click the icon of the group that you created.
6. In the left-hand window, click the port that you want to add to your group, and then click the right arrow to add the port to the group.

   To add multiple ports at once, press and hold CTRL as you click additional ports.

   Click and drag ports directly from the left-hand window to the port group to more quickly populate the group.

7. Click **OK** when you have finished adding ports to your group. The group appears in the **SAN Elements** tab under **PortGroups**. To view the contents of the group, click the group.

Configure File Transfer Options

1. From the **File** menu, select **Options...** The **Options** window opens, as shown in Figure 4-5.

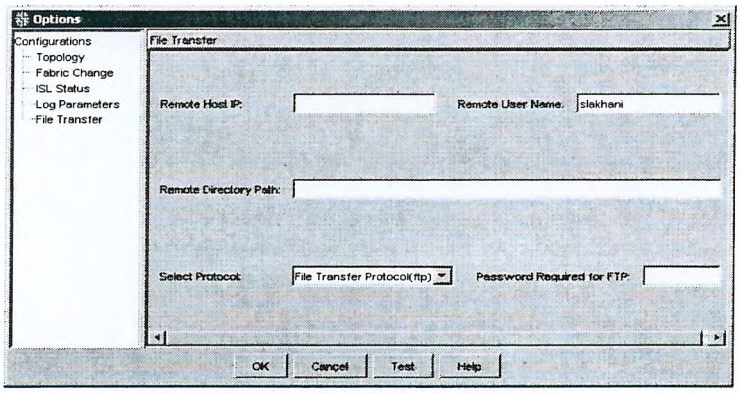


Figure 4-5 **Options Window**

2. The default view in the **Options** window is the File Transfer view. If the File Transfer view is not displayed, select **File Transfer** from the **Configurations** navigation tree (Figure 4-6).

Figure 4-6 **Options Window Configurations Tree**

3. In the **Remote Host IP** field, enter the IP address of your FTP server.
4. In the **Remote User Name** field, enter your login name.
5. In the **Remote Directory Path** field, enter a default FTP directory.

   Do not enter a file name, only a directory.

6. From the **Select Protocol** pull-down menu, select **File Transfer Protocol(ftp)**.
7. In the **Password Required for FTP** field, enter your password and click **OK**.
8. Click **Test** to ensure that you can access the FTP server specified. Fabric Manager will report success or failure.

In addition to validating connectivity to the FTP server, the Test button writes a temporary file to the FTP server. Write permissions must be set up properly on the specified path of the FTP server for the test to complete successfully.

---

9. Click **OK** to save settings.

Synchronize Time and Date across a Fabric

To synchronize time and date, you must choose fabrics, not switch groups.

1. Log in to the switches in the fabric that you want to synchronize. For more information, refer to *Log In To Multiple Switches Simultaneously* on page 4-8.
2. In the **SAN Elements** tab, click the fabric that you want to synchronize.
3. From the **Action** menu, select **Set Time...** The **Time** dialog box opens (Figure 4-1.)

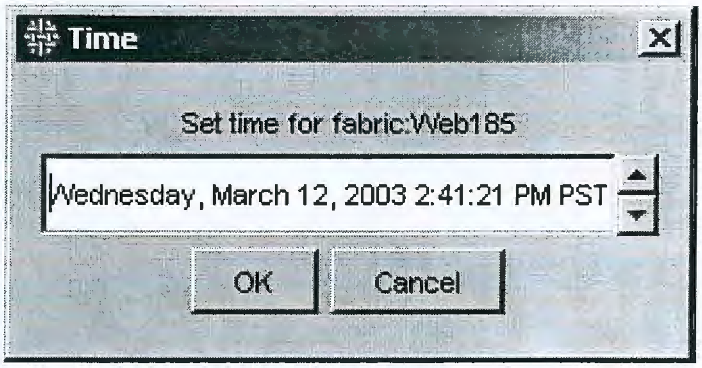


Figure 4-7 Time Dialog Box

4. To adjust the time or date, click the appropriate field in the **Time** dialog box and use the up and down arrows to iterate the value; then click **OK**.

Filter Elements

The Filter tab consists of the following three components:

- A text field
- A pull-down menu
- A **SAN Elements** field

To use the Filter tab:

1. From the pull-down menu, select an identifier. For more information, refer to *Filter Tab* on page 3-6.
2. In the text field, type text (letters, numbers, or symbols such as a period) that appears in the elements that you want to view. For example, to view elements that all include **`switch`** in the name, select **Name** from the pull-down menu and enter **switch** in the text field. To view elements that include **10.32** in the IP address, select **IP** from the pull-down menu and enter **`10.32`** in the text field.
3. Press ENTER. Every element that includes the text that you entered appears in the **SAN Elements** field.

Designate a Switch as a Core Switch

This procedure applies only to Core Edge topologies.

1. From the **SAN Elements** tab, click the switch that you want to designate.
2. From the **Actions** menu, select **Core Switch**. When you view the fabric that switch belongs to in Topology view and select the core-edge layout, your switch will appear as a core switch.

5 User Logins and Persistence

This chapter includes the following sections:

Introduction

Fabric Manager 4.0 requires that the user log in to use the software, and it stores user-specific settings for each user. Figure 5-1 shows the login dialog box.

Figure 5-1 **Fabric Manager Login Dialog Box**

Fabric Manager stores user settings when you exit, *not while you run the software*. Some persistent settings reside on the server and others reside on the client. If the client cannot access the server at exit, Fabric Manager alerts you that your settings will not persist.

When the client attempts to log in to the server, the server authenticates the client login. After the server authenticates the client, Fabric Manager launches and polls switches.

Log-In Scenarios

After you log in to Fabric Manager, connection problems may arise that can potentially interfere with the client. The following two scenarios occur most commonly:

1. While your client runs, your password changes on the server. When you try to close the client and store your settings, the client prompts you to enter your password. You must enter the new password to persist your data and close the client.
2. While your client runs, the server goes down. When you try to close the client, the client alerts you that you cannot persist your settings. The client gives you the option to close and lose your settings or wait until the server comes back up. When the server comes back up, you can exit and your settings persist.

Data That Persists

Fabric Manager stores the following user settings:

Locally

- Username
- Host name/server IP address of all servers you have successfully accessed
- Port numbers
- Browser path to launch Web Tools
- Dimensions of the Fabric Manager window
- Fabric Manager log directory path

Remotely

- Group definitions
- Discovered fabrics
- UI settings (view customizations, topology locations, and so on)
- Switch usernames and passwords

Persistence Files

Prior to Fabric Manager V4.0, two files stored user information locally. Table 5-1 lists and describes those files.

Table 5-1 Original Fabric Manager Persistence Files

File	Contents
`FabricManager.properties`	UI settings and configurable parameters
`FabricManager.xml`	Discovered fabrics and group definitions

To adapt to the client-server architecture of Fabric Manager V4.0, some of the content of the `FabricManager.properties` file now appears in a `FabricManagerUser.properties` file that resides on the server. Table 5-2 lists and describes the files that store user settings.

Table 5-2 Current Fabric Manager Persistence Files

File	Location	Contents
`FabricManager.properties`	client	Fabric Manager server usernames and port
`FabricManager.xml`	server	Discovered fabrics and group definitions
`LocationTable`	server	X and Y locations for topology nodes in Topology view
`FabricManagerUser.properties`	server	User interface settings such as window dimensions, known fabrics, file transfer settings, and default layout and link styles for the Topology view
`SwitchInfo.txt`	server	Login information with passwords encrypted

6

Grouping

This chapter includes the following sections:

Introduction

Logical *groups* consist of SAN elements (either switches or ports) that you select to monitor as a unit. When you click a group in the **SAN Elements** tab and select Summary view, you immediately see the status of the switches or ports that you added to the group. You can use groups to:

- Simplify monitoring
- Simplify management
- Organize switches by function, switch type, firmware version, or any other criteria that you choose
- Create functional hierarchies of groups

Create groups of similar switches and ports so you can monitor and configure them as a unit instead of individually. For instance, if you create a group of switches that run the same firmware, you can download new firmware to those switches as a group rather than one by one. Whenever you need to perform the same task on multiple switches, you can save time if you create a group and perform that task on the group. Examples of such tasks include:

- Multiple switch login
- Simultaneous firmware downloads
- Fabric-wide license key activations

A switch can appear in multiple groups at the same time

Groups persist on your server in your `FabricManager.xml` file. You can import and export groups so that multiple users can share group definitions.

Switches remain in a group even if you remove their source fabrics from Fabric Manager. That is, if switch X is in fabric Y and you add it to group Z, switch X remains in group Z even after you delete fabric Y from Fabric Manager.

Furthermore, when you look at a logical switch group in the Topology view, links will disappear if the switches that are in this group are no longer in the SAN Elements tab in Fabric Manager.

Best Practices

The following list describes valuable ways to use Fabric Manager groups:

- Create groups of switch model types or firmware versions to expedite firmware downloads.
- Group switches by function to monitor switches that belong to different departments or that serve as a backbone to the SAN.
- Group switches by physical location to monitor fabrics in disparate locations.
- Group switches by SAN island to monitor or update individual islands.
- Group switches by redundancy so you can maintain half of a fabric while the other half continues to carry traffic.
- Nest fabrics to drill down to the source of a problem. For instance, if you create a switch group for a campus and then nest within that switch group for departments, you can move down the hierarchy to determine the source of any status change.
- Create separate groups for monitoring and management to reduce unnecessary levels of nesting.
- Group ports by certain devices and hosts to more easily monitor those elements.
- Use groups to simplify the monitoring view of a large or complex fabric.

When you remove a switch from a fabric, you must remove that switch from all group definitions because Fabric Manager does not do so dynamically. For the same reason, if you replace the switch with a new switch, you must add that switch to all applicable group definitions.

Create a Group

With Fabric Manager, you can create a group of switches or a group of ports. Group switches together that serve similar purposes (for instance, all core switches or all switches that run the same firmware) and group ports together that serve similar purposes (for instance, all E_Ports).

Create SwitchGroups

A switch group consists of a collection of switch identifiers. After you create a group, you can click and drag that group during tasks to work with all switches at once. For instance, if you want to log in to all of the switches in a group, you can drag the group into the appropriate window so you do not need to select each individual switch. To create a group of switches, perform the following steps:

1. From the **File** menu, select **Groups, Edit Switch Groups...** The **Edit Switch Groups** dialog box appears.
2. Click the **SwitchGroups** icon in the right-hand window.

   The group that you create appears nested within the item that you click in this step. If you click an existing group instead of the **SwitchGroups** icon, your new group will appear as a subgroup of that group. After you create a group, you can click and drag it to a new location in the hierarchy.

3. Click **Create...** The **Create Group** dialog box appears.
4. Type a name for your group in the **Name** field and click **OK**.
5. Click the icon of the group that you created.
6. In the left-hand window, click the switch that you want to add to your group, and then click the right arrow to add the switch to the group.

   To add multiple switches at once, press and hold CTRL as you click additional switches, or simply click and drag any node in the tree to add the switches from that node.

   Click and drag switches directly from the left-hand window to the switch group to more quickly populate the group.

7. Click **OK** after you add switches to your group. The group appears in the **SAN Elements** tab under **SwitchGroups**. To view the contents of the group, click the group.

Create PortGroups

A port group essentially consists of a collection of port identifiers. After you create a group, you can click and drag that group during tasks to work with all ports at once. Perform the following steps to create a group of ports:

1. From the **File** menu, select **Groups, Edit Port Groups...** The **Edit Port Groups** dialog box appears.
2. Click the **PortGroups** icon in the right-hand window.

   The group that you create appears nested within the item that you click in this step. If you click an existing group instead of the **PortGroups** icon, your new group will appear as a subgroup of that group. After you create a group, you can click and drag it to a new location in the hierarchy.

3. Click **Create...** The **Create Group** dialog box appears.
4. Type a name for your group in the **Name** field and click **OK.**
5. Click the icon of the group that you created.
6. In the left-hand window, click the port that you want to add to your group, and then click the right arrow to add the port to the group.

   To add multiple ports at once, press and hold CTRL as you click additional ports.

   Click and drag ports directly from the left-hand window to the port group to more quickly populate the group.

7. Click **OK** when you have finished adding ports to your group. The group appears in the **SAN Elements** tab under **PortGroups**. To view the contents of the group, click the group.

Delete a Group

1. From the **File** menu, select **Groups, Edit {Switch | Port} Groups...** The **Edit {Switch | Port} Groups** dialog box appears.
2. In the right-hand window, navigate to the group that you want to delete and click that group.
3. Click **Delete**, and then click **OK**.

You can also select the group you want to delete from the SAN Elements tab and press **Delete** on your keyboard to delete a group.

Export Groups

When you create a group, that group exists in your `FabricManager.xml` file. To share your group definitions with other users, export the group so another user can import the group.

To export a group, perform the following steps:

1. From the **File** menu, select **Groups, Export...** The **Export** dialog box appears.
2. Click the **Browse...** button, navigate to the file you want to export the group to, and click **Open**.
3. Under the **SAN Elements** tab in the left window, click the group or groups that you want to add to the file.

You must select the parent group in order to import the parent group and all of its subgroups at a later time.

---

4. Click the arrow to add the group(s) to the file; then click **Save**.

Import a Group

Import groups to add group definitions from other users to your personal profile so you do not need to re-create the groups yourself. To import a group, perform the following steps:

1. From the **File** menu, select **Groups, Import...** The **Import from file:** dialog box opens.
2. Navigate to the file that contains the group that you want to import. Click the file, and then click **Open**. The groups in the file appear under the **SAN Elements** tab under the appropriate groups type.

7 Licensing

This chapter includes the following sections:

Introduction

Fabric Manager can display, store, load, and reload your license keys so that you do not lose them if your switch fails.

A Web Tools license must be installed on a switch in order for Fabric Manager to recognize the switch. All other licenses can be installed using Fabric Manager.

Import and Export License Keys

Export the license keys from healthy switches to a file so you can restore the licenses if switches fail. If for any reason you need to recover your license keys, import those keys from the file you created.

Export License Keys from Switches to a File

You can export the license keys of multiple switches to a single file. You can even export keys from different switches in different fabrics to one file. The file matches the license keys to the WWN of the appropriate switch so you can quickly and easily import the keys at any time. To export license keys to a file, perform the following steps:

1. From the **Tools** menu, select **Licensing, Load from Switch...** The **License Admin—Switch Selection** window appears.
2. In the **SAN Elements** tab, click the switches and/or fabrics with license keys that you want to export.
3. Click the right arrow to move elements that you selected into the right-hand window; then click **OK**. The **License Administration** window appears. If you have not already logged in to the switches, Fabric Manager prompts you to do so.
4. Click the **Switch** tab, then click the **Export to File** button. The **Export Licenses as an XML file** dialog box appears.
5. Select a directory, enter a name for the file, and click **Export**.

Do not open or manually edit this file.

Import License Keys from a File to a Switch

If you need to restore license keys to a switch, import the keys that you saved to a file. To import license keys from a file, perform the following steps:

1. From the **Tools** menu, select **Licensing, Import from File...** The **Import License—Select license file** window appears.
2. Navigate to your license key file, select it, and click **Open**. The **License Administration** window opens.
3. Click the licenses that you want to download and click **Download to Switch...** Fabric Manager loads the licenses to the appropriate switches. If you have not already logged in to the switches, Fabric Manager prompts you to do so.

Remove a License Key from a Switch

To remove a license key and disable the functionality of a licensed feature, perform the following steps:

1. From the **Tools** menu, select **Licensing, Load from Switch...** The **License Admin—Switch Selection** window appears.
2. In the **SAN Elements** tab, click the switches and fabrics with license keys that you want to remove.
3. Click the right arrow to move elements that you selected into the right-hand window; then click **OK**. The **License Administration** window appears.
4. Click the **Switch** tab, select the licenses that you want to remove, and click **Remove from Switch**.

8

Zoning

This chapter contains the following sections:

Introduction

Fabric Manager uses Web Tools to configure and administer zoning. This chapter provides high-level zoning instructions, and then goes into detail about zoning concepts and practices.

Specific Web Tools interfaces vary by firmware. Your interface and functionality may not match the interface that appears in the figures and examples in this chapter.

Zoning enables you to partition your SAN into logical groupings of devices that can access each other. For example, you can partition your SAN into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage. To configure zoning, you must use zones, aliases, and configurations.

Zone

A zone is a region within the fabric where switches and devices can communicate. A device can only communicate with other devices connected to the fabric within its specified zone. You can specify members of a zone based on the following identifiers:

- Alias names
- Switch domain and port area number pairs (for example, `2,20`)
- WWNs
- QuickLoop AL_PAs

Alias

An alias is a logical group of ports, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier by enabling you to configure zones using an alias rather than a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port area number pair (for example, `2,20`)
- WWN (device)
- QuickLoop AL_PAs (device)

Configuration

A configuration (often called a config) is a group of zones. Zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration with the following identifiers:

- Zone names
- QuickLoop names
- Fabric Assist (FA) zone names

Zoning Schemes

Various levels of zoning (or zoning *schemes*) isolate systems that have different operating environments. For example, you can create a zone of all ports connected to UNIX servers, or another zone of all ports connected to Windows servers. Zones limit access of devices to other devices connected to the fabric within the same zone.

Zones can be configured dynamically. They can vary in size depending on the number of fabric connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

Security

When you enable security, you can only access zoning with the primary FCS switch. The zoning icon does not appear on any other switch in the display. If you do not enable security, you can configure zoning from any switch.

Zoning Methods

Zoning methods determine what appears in the subsequent components of the **Zone Administration** window. You can use four methods to define members of a zone. Each method is considered either hard zoning or soft zoning. Hard zoning defines alias members exclusively with domain/port ID pairs or with WWNs. Soft zoning defines alias members with a mixture of port IDs and WWNs. Table 8-1 lists and describes the methods.

Table 8-1 Zoning Methods

Method	Description
Mixed Zoning	Enables you to define members using the port area number, device WWNs, QuickLoop AL_PAs. This method is considered soft zoning.
Port Zoning	Enables you to define members using port area number only. This method is considered hard zoning.
WWN Zoning	Enables you to define members of zone using device WWNs. This method is considered hard zoning.
AL_PA Zoning	Enables you to define members of zone using QuickLoop AL_PAs only. This method is considered hard zoning.

Zoning Method and Tabs Available

Depending on the zone method that you use, certain tabs may or may not be available on the **Zone Administration** window.

Table 8-2 Zone Methods and Tabs Table

Zone Level	Available Tabs
Mixed Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
Port Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
WWN Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
AL_PA Zoning	Alias, Zone, QuickLoop, Config

Access the Zone Administration Window

To access the **Zone Administration** window, perform the following steps:

1. From the **View** menu, select **Summary**.
2. In the **SAN Elements** tab, click the fabric that you want to view.
3. From the **Actions** menu, select **Zone Admin...** Web Tools launches and prompts you to log in.
4. Log in to Web Tools. The **Zone Administration** window opens.

View the Zone Configuration Summary

To view the **Zone Configuration summary**, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **File, Print Summary**. The **Zone Configuration summary** dialog box appears. An example of the **Zone Configuration summary** is shown in Figure 8-1.

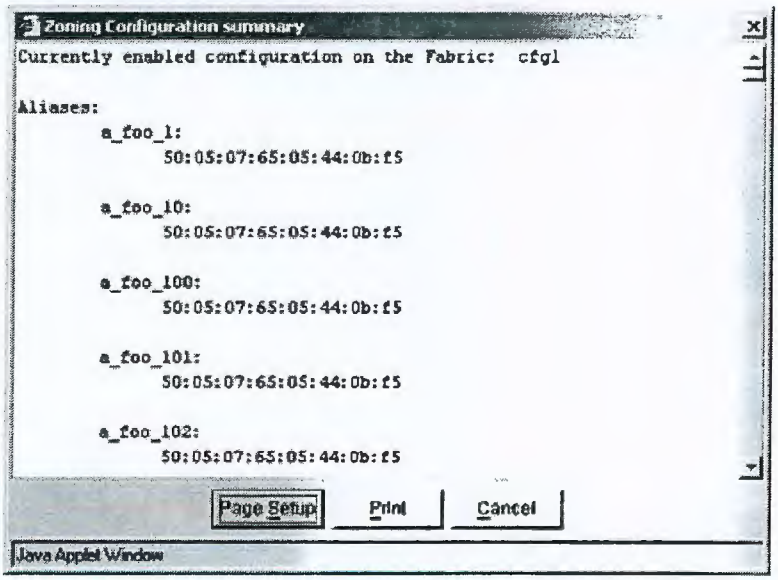


Figure 8-1 Zone Configuration Summary

Add a WWN in the Zoning Database

To add a WWN to the zoning database, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **Edit, Add a WWN**. The **Add WWN...** dialog box appears.
3. Enter a WWN value in the **WWN** field.
4. Click **OK**. The WWN is added to the zoning database and can be used as a member.

This WWN added does not need to currently exist in the fabric. This procedures enables you to configure a WWN as a member in a zone configuration before you add that device to the fabric.

Delete a WWN in the Zoning Database

To delete a WWN from the zoning database, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **Edit, Delete a WWN**. The **Delete WWN...** dialog box appears.
3. Enter a WWN value in the **WWN** field.
4. Click **OK**. The WWN is deleted from the zoning database and as a member from any alias or zone.

Replace a WWN in the Zoning Database

This procedure enables you to replace a WWN throughout the zoning database. This is helpful to exchange devices in your fabric, and allows you to easily maintain your current configuration. To replace a WWN in the zoning database, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **Edit** > **Replace a WWN**. The **Replace WWN...** dialog box appears.
3. Enter the WWN to be replaced in the **Replace** field.
4. Enter the new WWN in the **By** field.

5. Click **OK**. The old WWN is replaced in the zoning database by the new WWN, including within any alias or zone where the old WWN was a member.

Search for a Zone Member

To search for a zone member, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **Edit, Search Member**.
3. Type the zone member name in the **Member Name** field.
4. (Optional) Select one or more checkboxes to narrow the search.
5. Click the **Next** button to begin the zone member search.

Select a Zoning Method

The zoning method you choose determines how members appear in the various member selection windows. It also determines whether you are using hard zoning or soft zoning.

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. From the **View** pull-down menu, select one of the following:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

The zoning method that you choose determines how members appear in the various member selection windows. Refer to *Zoning Methods* on page 8-3 for more information.

Refresh Zoning

To refresh zoning, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. From the **View** menu, select **Refresh Zoning** to refresh the zoning database and delete any unsaved changes. You can view the current zoning database from the **Zone Configuration Summary** window. For more information, refer to *View the Zone Configuration Summary* on page 8-6.

Refresh the Fabric

To refresh the fabric, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. From the **View** menu, select **Refresh Fabric** to refresh the enabled zone configuration on the fabric and delete any unsaved changes. You can view the current zoning database from the **Zone Configuration Summary** window. For more information, refer to *View the Zone Configuration Summary* on page 8-6.

Enable a Configuration

The **Actions, Enable a Config** option enables a configuration that has previously been created (refer to *Create a Configuration* on page 8-21). A dialog box appears; select the desired configuration from the pull-down menu.

Several configurations can reside on a switch at once and you can quickly alternate between configurations. For instance, you may want to enable one configuration during the business hours and enable another overnight. You can only enable one zone configuration at a time.

To create a new configuration, refer to *Create a Configuration* on page 8-21. To enable a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.

2. Click the **View** pull-down menu.
3. Select the desired level of zoning.
4. Click the **Config** tab.
5. Select **Actions, Enable Config** to activate a configuration. The **Enable Config** dialog box appears (Figure 8-1).

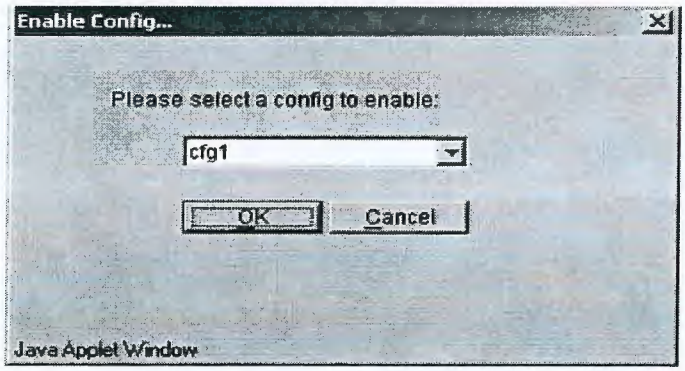


Figure 8-2 Enable Config... Dialog Box

Disable Zoning

The **Actions, Disable Zoning** option disables the enabled configuration. The **Disable Config** dialog box appears. When you disable the zoning feature, the fabric enters nonzoning mode and all devices can freely access other devices in the fabric.

When you disable the active configuration, the zoning feature is disabled on the fabric and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted however, only that there is no configuration active on the fabric. To disable zoning, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **Actions, Disable Zoning** to disable the current enabled configuration. The **Disable Config** warning appears.
3. Click **Yes** to disable the current configuration.

Save Changes to an Existing Configuration

To save changes to an existing configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Config** tab.
3. Make desired changes to configuration (refer to *Create a Zone* on page 8-15).

   You can make changes to a configuration that is currently enabled; changes will not appear until the configuration is disabled and reenabled.

4. Select the **Actions** , **Save Config Only** option.

   The configuration changes will be saved. Changes will not take effect until the configuration is reenabled.

   To enable the configuration, refer to *Enable a Configuration* on page 8-9.

Clear the Zoning Database

The following procedure disables any active configuration and deletes the entire zoning database:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select the **Actions, Clear All** option. The **Disable Config** warning appears.

CAUTION

This action will not only disable zoning on the fabric, but will deleted the entire zoning database.

3. Click the **Yes** button to disable the current configuration.

Create an Alias

To create an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select the **View** menu to determine the method used to view members. The different methods are as follows:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

   The member view method you choose determines how members are displayed in the **Member Selection List** window. Refer to *View Menu* on page H-5 for more information.
3. Click the **Alias** tab (selected by default).
4. Click the **Create Alias** button. The **Create New Alias** dialog box appears.
5. Enter a name for the new alias.
6. Click **OK**.
7. Click on any "+" signs in the **Member Selection List** to view the nested elements. The choices available in the **Member Selection List** depend on the selection that you made in the **View** menu.
8. Highlight an element in the **Member Selection List** that you want to include in your alias. The **Add Member** button becomes active.
9. Click the **Add Member** button to add alias members. Selected members move to the **Alias Members** window.
10. Repeat step 7 and step 8 to add more elements to your alias.
11. Use the **Add Other** button to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional).

    The new alias appears in the **Name** pull-down list.

Modify the Members of an Alias

To modify the members of an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Alias** tab (selected by default).
3. From the **Name** pull-down menu, select the alias you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your alias; or, highlight an element in the **Alias Members** field that you want to delete.
5. Click the **Add Member** button to add an alias member or click the **Remove Member** button to remove an alias member.

Delete an Alias

To delete an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Alias** tab (selected by default).
3. From the **Name** pull-down menu, select the alias you want to delete.
4. Click **Delete.** The **Confirm Deleting Alias** dialog box opens.
5. Click **OK** to delete the alias from the zoning database.

Rename an Alias

To rename an alias, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Alias** tab (selected by default).
3. From the **Name** pull-down menu, select the alias you want to rename.
4. Click **Rename**. The **Rename an Alias** dialog box appears.
5. Enter a new alias name and click **OK**.

Create a Zone

To create a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select the **View** menu to determine the method used to view members. The different methods include the following:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

   The member view method that you choose determines how members are displayed in the **Member Selection List** window. For more information, refer to *View Menu* on page H-5.
3. Select the **Zone** tab.
4. Click **Create**. The **Create New Zone** dialog box appears.
5. Enter a name for the new zone and click **OK**.
6. Click on any "+" signs in the **Member Selection List** to view the nested elements. The choices available in the **Member Selection List** depend on the selection made in the **View** menu.
7. Highlight an element in the **Member Selection List** that you want to include in your zone. The **Add Member** button becomes active.
8. Click the **Add Member** button or use drag and drop to add zone members. Selected members move to the **Zone Members** window.
9. Repeat step 7 and step 8 to add more elements to your zone.

Use the **Add Other** button to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional). The new zone appears in the **Name** pull-down menu.

Modify the Members of a Zone

To modify the members of a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Zone** tab.

3. From the **Name** pull-down menu, select the zone that you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your zone; or, highlight an element in the **Zone Members** field that you want to delete.
5. Click the **Add Member** button to add a zone member or click the **Remove Member** button to remove a zone member.

Delete a Zone

To delete a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Zone** tab.
3. From the **Name** pull-down menu, select the zone you want to delete.
4. Click **Delete**. The **Confirm Deleting Zone** dialog box opens.
5. Click **OK.**

Rename a Zone

To rename a zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Zone** tab.
3. From the **Name** pull-down menu, select the zone you want to rename.
4. Click **Rename**. The **Rename a Zone** dialog box appears.
5. Enter a new zone name and click **OK**.

Create a QuickLoop

To create a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. From the **View** menu, select one of the following methods:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

   The method that you choose determines how members appear in the **Member Selection List** window. For more information, refer to *View Menu* on page H-5.
3. Click the **QuickLoop** tab.
4. Click **Create**. The **Create New QuickLoop** dialog box appears.
5. Enter a name for the new QuickLoop and click **OK**.
6. Highlight an element in the **Member Selection List** that you want to include in your QuickLoop. (Click on any "+" signs in the **Member Selection List** to view the nested elements. The choices available in the **Member Selection List** depend on the selection made in the **View** menu.) The **Add Member** button becomes active.

   There is a limit of two members per QuickLoop.

7. Click the **Add Member** button to add QuickLoop members. Selected members move to the **QuickLoop Members** field.
8. Repeat step 6 and step 7 to add more elements to your QuickLoop.
9. Use the **Add Other** button to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional).

   The new QuickLoop appears in the **Name** pull-down menu.

Modify the Members of a QuickLoop

To modify the members of a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **QuickLoop** tab.
3. From the **Name** pull-down menu, select the QuickLoop you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your QuickLoop, or highlight an element in the **QuickLoop Members** that you want to delete.
5. Click the **Add Member** button to add a QuickLoop member or click the **Remove Member** button to remove an QuickLoop member.

Delete a QuickLoop from the Database

To delete a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **QuickLoop** tab.
3. From the **Name** pull-down menu, select the QuickLoop you want to delete.
4. Click **Delete**. The **Confirm Deleting QuickLoop** dialog box opens.
5. Click **OK**.

Rename a QuickLoop

To rename a QuickLoop, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **QuickLoop** tab.
3. From the **Name** pull-down menu, select the QuickLoop you want to rename.
4. Click **Rename**. The **Rename a QuickLoop** dialog box appears.
5. Enter a new QuickLoop name.
6. Click **OK** button.

Create a Fabric Assist Zone

To create a Fabric Assist zone, perform the following steps:

This example uses the Mixed Zone level.

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Enter the admin level user name and password.
3. From the **View** menu, select **Mixed Zoning**. (You can select any view except for the Devices view.) The **Mixed View** tab appears.
4. Click the **Fabric Assist** tab.
5. Click **Create**. The **Create New FA** dialog box appears.
6. Enter a name for the new FA zone and click **OK**. (A fabric host is required.)
7. Highlight the desired Fabric Assist zone members from the **Member Selection List**.
8. Click the **Add Member** button. The new members appear in the **Fabric Assist Members** window. The newly created FA zone also appears in the **Config** tab.

Modify the Members of a Fabric Assist Zone

To modify the members of a Fabric Assist zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Fabric Assist** tab.
3. From the **Name** pull-down menu, select the Fabric Assist Zone that you want to modify.
4. Highlight an element in the **Member Selection List** that you want to include in your Fabric Assist zone; or, highlight an element in the **Fabric Assist Zone Members** field that you want to delete.
5. Click the **Add Member** button to add a Fabric Assist zone member or click the **Remove Member** button to remove an Fabric Assist zone member.

Delete a Fabric Assist Zone

To delete a Fabric Assist zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Fabric Assist Zone** tab.
3. From the **Name** pull-down menu, select the Fabric Assist zone you want to delete.
4. Click **Delete.** The **Confirm Deleting Fabric Assist Zone** dialog box opens.
5. Click **OK**.

Rename a Fabric Assist Zone

To rename a Fabric Assist zone, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Fabric Assist** tab.
3. From the **Name** pull-down menu, select the Fabric Assist zone that you want to rename.
4. Click **Rename**. The **Rename a Fabric Assist Zone** dialog box appears.
5. Enter a new Fabric Assist zone name and click **OK**.

Create a Configuration

To create an configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. From the **View** menu, select one of the following methods:
   - Mixed Zoning,
   - Port Zoning,
   - WWN Zoning,
   - AL_PA Zoning.

   The member view method that you choose determines how members appear in the **Member Selection List** window. Refer to *View Menu* on page H-5 for more information.
3. Click the **Config** tab.
4. Click **Create**. The **Create New Config** dialog box appears.
5. Enter a name for the new configuration and click **OK**.
6. Click on any "+" signs in the **Member Selection List** to view the nested elements.
7. Highlight an element in the **Member Selection List** that you want to include in your configuration. The **Add Member** button becomes active.
8. Click the **Add Member** button to add configuration members. Selected members move to the **Config Members** field.
9. Repeat step 7 and step 8 to add more elements to your configuration.
10. Select the **Actions** > **Save Config Only** option. The new configuration appears in the **Name** pull-down menu. To enable the configuration, refer to *Enable a Configuration* on page 8-9.

Any changes made to the currently enabled configuration will not appear until the configuration is reenabled.

Modify the Members of a Configuration

To modify the members of a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Config** tab.
3. From the **Name** pull-down menu, select the configuration that you want to modify.
4. Click an element in the **Member Selection List** that you want to include in your configuration or click an element in the **Config Members** that you want to delete.
5. Click the **Add Member** button to add a configuration member or click the **Remove Member** button to remove a member from a configuration.

   You can make changes to a configuration that is currently enabled; changes will not appear until the configuration is disabled and reenabled.

6. Select the **Actions, Save Config Only** option.

   The configuration changes will be saved. Changes will not take effect until the configuration is reenabled.

   To enable the configuration, refer to *Enable a Configuration* on page 8-9.

Delete a Configuration

You cannot delete a currently enabled configuration.

To delete a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Config** tab.
3. From the **Name** pull-down menu, select the configuration you want to delete.
4. Click **Delete**. The **Confirm Deleting Config** dialog box opens.
5. Click **OK**.

Rename a Configuration

To rename a configuration, perform the following steps:

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Select **Config**.
3. From the **Name** pull-down menu, select the configuration you want to rename.
4. Click **Rename**. The **Rename a Config** dialog box appears.
5. Enter a new **Config** name and click **OK**.

   You can make changes to a configuration that is currently enabled; changes will not appear until the configuration is disabled and reenabled.

6. Select the **Actions** > **Save Config Only** option.

   The configuration changes will be saved. Changes will not take effect until the configuration is reenabled.

   To enable the configuration, refer to *Enable a Configuration* on page 8-9.

Create a Configuration Analysis Report

1. Access the **Zone Administration** window. For more information, refer to *Access the Zone Administration Window* on page 8-5.
2. Click the **Config** tab.
3. From the **Name** pull-down menu, select a configuration to analyze.

4. Click the **Analyze Config** button. An analysis window appears. An example of an analysis report is shown in <Link>Figure 8-3.

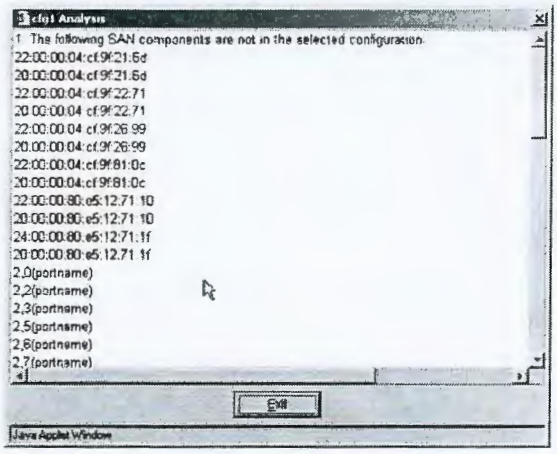


Figure 8-3 Analyze Config Report Example

5. View the Configuration Analysis. A report appears that lists the following:
   - SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration.
   - SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration but not in the fabric.

9 Fabric Watch

This chapter contains the following sections:

Introduction

Fabric Watch software monitors the performance and status of switches and can alert SAN administrators when problems arise. The realtime alerts from Fabric Watch software help SAN administrators solve problems before they become costly failures. Fabric Manager launches Web Tools to configure Fabric Watch, so the options that Fabric Manager provides depend on the individual switch and the firmware that runs on the switch. SAN managers can configure Fabric Watch software to monitor any of the following:

- Fabric events (such as topology reconfigurations and zone changes)
- Physical switch conditions (such as fan speeds, power supply status, and chassis temperature)
- Port behavior and availability (such as state changes, errors, and performance)
- Small form factor pluggables (SFPs)
- Security events (violations and attempted violations)

Specific Web Tools interfaces vary by firmware. Your interface and functionality may not match the interface that appears in the figures and examples in this chapter.

Fabric Watch is an optional feature on the Connectrix B-Series.

Fabric Watch Terms

Table 9-1 lists and defines Fabric Watch terms.

Table 9-1 Fabric Watch Terms and Definitions

Term	Definition
Threshold	A configuration of boundaries, traits, and alarms that determine when an event occurs and how Fabric Watch responds to the event.
Boundary	A limit (high or low) on the acceptable value of a counter.
Counter	The value of the behavior of an element. For instance, the temperature of an SFP or the number of CRC errors.
Trait	Behavioral characteristic of a threshold.
Alarm	Response to an event.
Element	Any component or condition of a switch that Fabric Watch monitors.
Event	Behavior of a counter that can trigger an alarm. The following events can trigger an alarm: ◆ A counter value rises above a high boundary (above event) ◆ A counter value falls below a low boundary (below event) ◆ A counter value rises above or falls below a range of acceptable values (exceeded event) ◆ The value of a counter changes (changed event) ◆ A counter value returns from a value outside of an acceptable range to a value within the acceptable range (in-between event)

How Fabric Watch Works

With Fabric Watch software, SAN administrators can place limits, or *boundaries*, on the behavior of different switch and fabric *elements*. Fabric Watch then monitors these behavior variables, or *counters*, and can issue an alarm when a counter triggers an *event*. An alarm may send an e-mail to the SAN administrator or forward all error information to a proxy switch; the response depends upon how the administrator configures Fabric Watch.

How to Use Fabric Watch

To use Fabric Watch:

- Choose elements that you want to monitor.
- Place limits on the acceptable values of those elements (configure threshold boundaries).

  This step only applies when you monitor counters that must remain within boundaries. If you want Fabric Watch to alert you whenever a counter changes, configure an alarm for a Changed event.

- Choose if and how Fabric Watch alerts you to errant values (configure threshold alarms).
- Choose whether Fabric Watch continues to alert you to persistent errant values (configure threshold traits).
- Enable the thresholds that you configured (configure threshold traits).

Access Fabric Watch

To access Fabric Watch, perform the following steps:

1. Verify that the switch that you want to configure includes a Fabric Watch license. For more information, refer to Chapter 7, *Licensing*.
2. In the **SAN Elements** tab, click the switch that you want to configure.
3. From the **Actions** menu, select **Fabric Watch...** A separate browser window opens and prompts you to log in to the switch. After you successfully log in, the Web Tools **Fabric Watch** window opens.

View Alarms

To view Fabric Watch alarms, perform the following steps:

1. Launch Fabric Watch (refer to *Access Fabric Watch* on page 9-5).
2. In the **Fabric Watch** navigation tree, click the class that you want to check for alarms.
3. Click the **Alarm Notification** tab.
4. From the **Select Area** pull-down menu, select the area that you want to check for alarms. All alarms for that area appear. For troubleshooting responses to alarms, refer to the Fabric Watch documentation for your firmware.

Configure Threshold Boundaries and Alarms

Configure Fabric Watch boundaries and alarms to designate the circumstances that trigger events and how Fabric Watch responds to those events. To configure threshold boundaries and alarms, perform the following steps:

1. Launch Fabric Watch (refer to *Access Fabric Watch* on page 9-5).
2. In the **Fabric Watch** navigation tree, click the class that you want configure.
3. Click the **Threshold Configuration** tab.
4. Click the **Area Configuration** subtab.
5. From the **Select Area** pull-down menu, select the area that you want to configure.
6. Enter custom values in the trait fields (such as **Unit, High**, and **Low**) in the **Boundary Settings (Default Settings in Parentheses)** partition.
7. From the **Select Boundary Level** pull-down menu in the **Boundary** partition, select **Custom**.
8. In the **Alarm Notification Mechanisms (Default Mechanisms in Parentheses)** partition, select the events that you want to trigger an alarm. You can choose from the following events:
   - Changed
   - Exceeded
   - Below
   - Above
   - In-Between

   After you select an event, you can select alarms to notify you when the event occurs.
9. Select the checkbox of each alarm that you want to associate with the event(s) that you selected.
10. From the **Select Alarm Level** pull-down menu in the **Alarm Setting** partition, select **Custom**.
11. Click **Apply**.

For your alarms to function once you configure them, you must enable alarms (refer to *Enable/Disable Thresholds* on page 9-7).

Configure E-Mail Alert

To configure the e-mail alert alarm, perform the following steps:

1. Launch Fabric Watch (refer to *Access Fabric Watch* on page 9-5).
2. Click the **e-mail Configuration** tab.
3. In the **Mail To:** field, enter the e-mail address of the administrator who receives e-mail alerts.
4. In the **Mail Status** partition, click the **Enabled** radio button; then click **Apply**.

Enable/Disable Thresholds

Perform the following steps to enable or disable alarms:

1. Launch Fabric Watch (refer to *Access Fabric Watch* on page 9-5).
2. In the **Fabric Watch** navigation tree, click the class with the alarms that you want to enable or disable.
3. Click the **Threshold Configuration** tab.
4. From the **Select Area** pull-down menu, select the area with the alarms that you want to enable or disable.
5. Click the **Element Configuration** sub-tab.
6. From the **Select Element** pull-down menu, select the element that you want to enable or disable.
7. In the **Status** partition, click the **Enabled** or **Disabled** radio button.
8. Click **Apply**. Web Tools enables or disable the element.

Configure Threshold Traits

Configure threshold traits to designate if and when Fabric Watch monitors an element. To configure threshold traits, perform the following steps:

1. Launch Fabric Watch (refer to *Access Fabric Watch* on page 9-5).
2. In the **Fabric Watch** navigation tree, click the class that you want to configure to a different behavior.
3. Click the **Threshold Configuration** tab.
4. From the **Select Area** pull-down menu, select the area that you want to configure to a different behavior.
5. Click the **Element Configuration** sub-tab.
6. From the **Select Element** pull-down menu, select the element that you want to configure to a different behavior.
7. Click the **Triggered** radio button to configure triggered behavior or click the **Continuous** radio button to configure continuous behavior.

   If you click the **Continuous** radio button, enter a time interval in the **Time Interval** pull-down menu, or select an interval from the pull-down menu.

8. Click **Apply**.

View an Alarm Configuration Report

View an alarm configuration report to review information about Fabric Watch settings and thresholds. For detailed information on the configuration report, refer to *Configuration Report Tab* on page I-6. To view the configuration report, perform the following steps:

1. Launch Fabric Watch (refer to *Access Fabric Watch* on page 9-5).
2. In the **Fabric Watch** navigation tree, click the class that you want to configure to a different behavior.
3. Click the **Threshold Configuration** tab.
4. From the **Select Area** pull-down menu, select the area that you want to view.
5. Click the **Configuration Report** sub-tab.

10 Security Management

This chapter contains the following sections:

Introduction

Fabric Manager provides a GUI interface to manage security once you enable security with command-line commands. For Fabric Manager to access secure switches, you must configure your security policies (at the command line) as follows:

- You must add the IP address of any host that runs the Fabric Manager server to the IP policy of your fabric. The server cannot communicate with the fabric if you do not include this IP address. (This holds true whether or not the machine also runs the Fabric Manager client.)
- You must add every client that you want to run the API to the API policy of your fabric.

Fabric Manager lets you configure SAN security to restrict sensitive operations to a few *trusted* switches. It allows administrators to designate a small number of switches, known as Fabric Configuration Servers (FCS), to perform fabric-wide management operations. Security acts on a policy basis, which means you can selectively choose what functionality a switch can access.

You can configure numerous aspects of security with Fabric Manager in the **Security Admin** window (Figure 10-1).

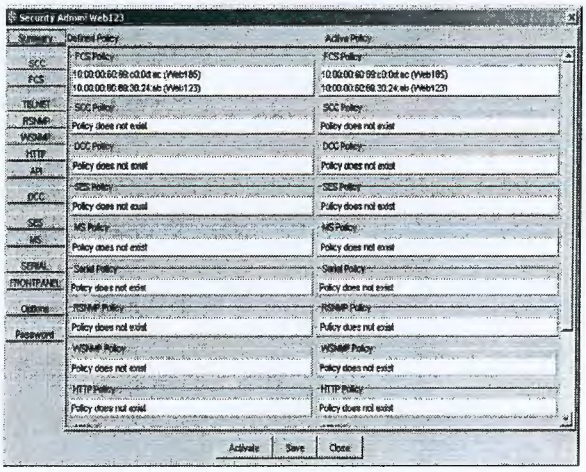


Figure 10-1 Security Admin Window

For detailed information on security, refer to the *Secure Fabric OS User Guide*.

To Administer Security with Fabric Manager:

1. Enable security on a fabric
2. Administer the following options:
   - Create, remove, or add switch members in the Switch Connection Controls (SCC) policy

     The SCC policy does not exist when you first enable security. You must create and add members with Fabric Manager.

   - Add, remove, or move FCS members
   - Add or remove switches from the Telnet, RSNMP, WSNMP, HTTP, and API policies

     Remove all switches to shut down an access method

   - For device connection control (DCC) policies, configure multiple policies with unique names

For EMC Connectrix switches, please check the *EMC Support Matrix* and firmware release notes for updated information regarding support of this feature.

View and Configure Security Policy Options

To configure security on a secure fabric, perform the following steps:

1. Log in to the primary FCS of the secure fabric that you want to configure.
2. From the **SAN Elements** tab, select the fabric that you want to secure.
3. From the **Actions** menu, select **Security**. The **Security Admin** window appears.
4. Click the **Summary** tab to view your defined policies and active policies.

When you make changes in the **Security Admin** window, you have the option to click **Apply** to activate your changes, or **Save** to store your updates but not activate them.

Add a Switch to a Secure Fabric

To add a switch to a secure fabric, you must define that switch in the SCC policy. The SCC policy defines all switches in the fabric (FCS and non-FCS). You cannot add a new switch to a fabric if you do not add that switch to the SCC policy. To add a switch to a secure fabric, perform the following steps:

1. From the **SAN Elements** tab, choose the fabric that you want to secure.
2. From the **Actions** menu, select **Security**.
3. Click the **SCC** tab.
4. Enter the new switch WWN in the empty field.

   When switches already exist in the fabric, you can specify a * (do not include quotes) in place of a switch WWN. When added, the * will expand to include all switches in the fabric.
5. Select **Add Switch** to move the switch to the **Fabric Switches** window.
6. Select **Activate** to add the new switch to secure fabric, implement the security policy, and exit the window.

Configure SCC Policy Options

The SCC policy defines all switches in the secure fabric (FCS and non-FCS). To create a SCC policy, perform the following steps:

1. From the **Security Admin** window, click the **Switch Connection Controls (SCC)** tab.
2. Click **Create Policy**. The WWN of all current switches in the fabric appears in the **Fabric Switches** field.
3. In the **Enter New Switch WWN** field, enter the WWN of a switch that you want to include in the policy, or enter * to add all switches in the fabric.
4. Click the **Add Switch** button.
5. Repeat step 3 and step 4 to add more switches.

   All switches within a fabric must be included in the SCC policy, or else the excluded switches will be segmented out from the fabric.

6. Click **Save** to save your changes but not apply them, or click **Activate** to save and apply your changes.

To edit a SCC policy, click the **SCC** tab and perform any of the following actions:

- To delete the policy, click **Delete Policy**.
- To add WWNs to the policy, enter the WWN of another switch in the **Enter New Switch WWN** field and click **Add Switch**. Repeat this step for every WWN that you want to add.
- To remove WWNs from the policy, click a WWN in the **Fabric Switches** field, and then click **Remove Switch**.

Configure FCS Options

Switches in your FCS policy serve as *trusted switches*. The first switch in the policy serves as the primary FCS (from which you can configure your fabric), and each subsequent switch serves as a backup FCS. The order in which switches appear in the policy represents the order in which each backup switch will take over as primary FCS if the preceding primary FCS fails. To add an FCS to your fabric, perform the following steps:

1. From the **Security Admin** window, click the Fabric Configuration Servers (**FCS**) tab.
2. Select a switch from the **Available Switch List** column and use the **Add FCS** button to add it to the **FCS Switch List**. The switches appear in the order in which they will become a primary FCS switch if the primary FCS fails.
3. (Optional) Click **Add Others...** to open the **Enter WWN** dialog box. Enter a switch WWN in this dialog box to add the switch to the **FCS Switch List**.
4. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your **FCS Switch List**, perform any of the following actions:

- To remove a switch from the FCS list, click the WWN of a switch in the FCS Switch List and click **Remove FCS**.
- To change the order of the FCS switches (to determine which switch will become the next primary FCS), click a switch and click the up or down buttons beneath the **FCS Switch List** field.

Configure Telnet Policy Options

The Telnet policy contains a list of IP addresses and/or subnets that can establish Telnet connections to any switch in the fabric. Telnet attempts from any IP address or subnet that do not appear in the policy will fail. If you create an empty policy, you prevent all Telnet access to your fabric. To create a Telnet policy, perform the following steps:

1. Click the **TELNET** tab in the **Security Admin** window.
2. Click **Create Policy**.
3. In the **Enter IP Address** field, type the IP address of a switch that you want to include in the policy.
4. Click **Add IP>**. The IP address appears in the **Permitted Access Points** field.
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your Telnet policy, perform any of the following actions:

- To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
- To delete the Telnet policy, click **Delete Policy**.

Configure RSNMP Policy Options

You cannot create a RSNMP policy without a WSNMP policy already present.

Configure the RSNMP policy to limit SNMP access to specific, trusted management stations in your environment. To create a RSNMP policy, perform the following steps:

1. Click the **RSNMP** tab in the **Security Admin** window.
2. Click **Create Policy**.
3. Type the IP address of a switch that you want to include in the policy in the **Enter IP Address** field.
4. Click **Add IP** . The IP address appears in the **Permitted Access Points** field.
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your RSNMP policy, perform any of the following actions:

- To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
- To delete the RSNMP policy, click **Delete Policy**.

Configure WSNMP Policy Options

Configure the WSNMP policy to limit SNMP access to specific, trusted management stations in your environment. When you add a member to the WSNMP policy, that member automatically gains RSNMP access. To create a WSNMP policy, perform the following steps:

1. Click the **WSNMP** tab in the **Security Admin** window.
2. Click **Create Policy**.
3. In the **Enter IP Address** field, type the IP address of a switch that you want to include in the policy.
4. Click **Add IP**. The IP address appears in the **Permitted Access Points** field.
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your WSNMP policy, perform any of the following actions:

- To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
- To delete the WSNMP policy, click **Delete Policy**.

Configure HTTP Policy Options

Configure the HTTP policy to grant access to IP addresses and/or subnets so they can establish HTTP connections to the switches in the fabric.

The IP address of your Fabric Manager client must appear in this policy or you cannot access the fabric with Fabric Manager.

To create a HTTP policy, perform the following steps:

1. Click the **HTTP** tab in the **Security Admin** window.
2. Click **Create Policy**.
3. In the **Enter IP Address** field, type the IP address of a switch that you want to include in the policy.
4. Click **Add IP**. The IP address appears in the **Permitted Access Points** field.
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your HTTP policy, perform any of the following actions:

- To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
- To delete the HTTP policy, click **Delete Policy**.

Configure API Policy Options

Create an API policy to control the workstations that can use the API to write to the fabric.

If you use Fabric Manager to update the API policy to disable API access from the current host (either by creating an empty policy or by specifically excluding this host from the API policy list), the security transaction will be locked and can take up to two hours before Fabric OS releases the security transaction. You cannot modify the policies until the security transaction is released.

To create a API policy, perform the following steps:

1. Click the **API** tab in the **Security Admin** window.
2. Click **Create Policy**.
3. In the **Enter IP Address** field, type the IP address of a switch that you want to include in the policy.
4. Click **Add IP**. The IP address appears in the **Permitted Access Points** field.
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your API policy, perform any of the following actions:

- To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
- To delete the API policy, click **Delete Policy**.

Configure DCC Policy Options

Configure DCC policies to bind device ports to specific switch ports. With Fabric Manager, you can create and configure multiple DCC policies with unique names. Populate DCC policies with switch and device WWNs. To create a DCC policy, perform the following steps:

1. From the **Security Admin** window, click the **DCC** tab.
2. Click the **Create Policy** button. The **Enter DCC Policy** dialog box appears.
3. In the **Enter Policy Name** field, enter a name for a new policy and click **Create**. The name appears in the **Policy** pull-down menu.
4. Use the **Add member**, **Remove member**, and **Add Device WWN...** buttons to populate the policy.
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your DCC policies, perform any of the following actions for each individual DCC policy:

- To remove a DCC policy, select the policy from the **Policy:** pull-down menu and click **Delete Policy**.
- To rename a DCC policy, select the policy from the **Policy:** pull-down menu and click **Rename Policy**.
- To change the contents of a DCC policy, select the policy from the **Policy:** pull-down menu, and then select WWNs from the appropriate window and click **Add member** to add the WWN or **< Remove member** to remove the WWN from the policy. To add a WWN that does not appear in the **Switches and Devices** tab, click **Add Device WWN...** and enter the WWN that you want to add.

Configure SES Policy Options

Create an SES policy to allow device ports to access SES. With Fabric Manager, you can create and configure multiple SES policies with unique names. Populate SES policies with switch and device WWNs. SES and MS policies are device-based. To create a SES policy, perform the following steps:

1. From the **Security Admin** window, click the **SES** tab.
2. Click **Create Policy**. The WWN of a device that connects to the fabric appears in the **Permitted Access Points** field.
3. Select a device from the **Permitted Access Points** field.
4. Click **Add Device.**
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your SES policy, perform any of the following actions:

- To delete the policy, click **Delete Policy.**
- To add a device to the policy, click the device in the **Available Access Points** field, and then click **Add Device**. (Click **Save** or **Activate** as appropriate.)
- To remove a device from the policy, click the device in the **Permitted Access Points** field, and then click **Remove Device**. (Click **Save** or **Activate** as appropriate.)

Configure MS Policy Options

Create an MS policy to allow trusted fabric-connected devices to access the management server. With Fabric Manager, you can create and configure multiple MS policies with unique names. Populate MS policies with switch and device WWNs. MS and MS policies are device-based. To create an MS policy, perform the following steps:

1. From the **Security Admin** window, click the **MS** tab.
2. Click **Create Policy**. The WWN of a device that connects to the fabric appears in the **Permitted Access Points** field.
3. Select a device from the **Permitted Access Points** field.
4. Click **Add Device.**
5. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your MS policy, perform any of the following actions:

- To delete the policy, click the **Delete Policy**.
- To add a device to the policy, click the device in the **Available Access Points** field, and then click **Add Device**. (Click **Save** or **Activate** as appropriate.)
- To remove a device from the policy, click the device in the **Permitted Access Points** field, and then click **Remove Device**. (Click **Save** or **Activate** as appropriate.)

Configure Serial Policy Options

Create a serial policy to grant serial port access to specific switches. To create a serial policy, perform the following steps:

1. From the **Security Admin** window, click the **SERIAL** tab.
2. Click **Create Policy**. You have now created an empty policy, which denies serial access to *all switches in the fabric*.

CAUTION

If you create empty policies in the serial, Telnet, HTTP, and API policies simultaneously, you can no longer manage security.

3. Click a switch in the **Available Access Points** field and click **Add Switch >** to add it to your policy. Repeat this step for each switch that you want to add.
4. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your serial policy, perform any of the following actions:

- To delete the policy, click **Delete Policy**.
- To add a switch to the policy, click the switch in the **Available Access Points** field, and then click **Add Switch**. (Click **Save** or **Activate** as appropriate.)
- To remove a switch from the policy, click the switch in the **Permitted Access Points** field, and then click **Remove Switch**. (Click **Save** or **Activate** as appropriate.)

Configure Front-Panel Policy Options

Configure the front-panel policy to enable front-panel access to specific DS-16B switches. To create a front-panel policy, perform the following steps:

1. From the **Security Admin** window, click **FRONTPANEL** tab.
2. Click **Create Policy**. You have now created an empty policy, which denies front panel access to *all switches in the fabric*.
3. Click a switch in the **Available Access Points** field and click **Add Switch >** to add it to your policy. Repeat this step for each switch that you want to add.
4. Click **Save** to save your changes but not apply them, or click **Activate** to apply your changes.

To make changes to your front panel policy, perform any of the following actions:

- To delete the policy, click **Delete Policy**.
- To add a switch to the policy, click the switch in the **Available Access Points** field, and then click **Add Switch**. (Click **Save** or **Activate** as appropriate.)
- To remove a switch from the policy, click the switch in the **Permitted Access Points** field, and then click **Remove Switch**. (Click **Save** or **Activate** as appropriate.)

Configure No Node WWN Zoning

Fabric Manager provides a tab that lets you enable or disable No Node WWN Zoning. When you enable this feature, security becomes port-oriented. Devices have port and node WWNs. When you disable node zoning, you ensure that devices with multiple ports cannot access secure fabrics with node WWNs. You must add individual port WWNs to your policies for devices to access your secure fabric. To configure No Node WWN Zoning, perform the following steps:

1. From the **Security Admin** window, click the **Options** tab.
2. Select the **No Node WWN Zoning** checkbox to enable this policy.

Change the FCS or Non-FCS Admin Security Password

To change the password that implements security, perform the following steps:

1. From the **Security Admin** window, click the **Password** tab.
2. In the **FCS Administrator Password** field, enter the appropriate password.
3. In the **New Password** field, enter your new password.
4. In the **Verify** field, enter your new password again.
5. Select the **FCS Switches** or **non-FCS Switches** radio button.

   Select the **FCS switches** radio button to make a password change to the secure access switch(es).

6. Click **Change Password**.

11 Call Home

This chapter includes the following sections:

Introduction

The Call Home feature of Fabric Manager continuously monitors the status of switches and sends a *call home* e-mail message to user-defined e-mail addresses when a triggering condition occurs. The e-mail message should be directed to a storage administrator or other person in the user account responsible for monitoring and managing the storage infrastructure. Triggering conditions include the following:

- Switch status change (consists of any change that registers in `switchstatuspolicyshow` command output)
- Switch reboot
- Switch unreachable (experiences a complete loss of connectivity)

Call Home, when enabled, automatically sends an e-mail alert in the event of status change or a reboot. You must configure Call Home to:

- Send an alert when the host cannot contact the switch (`switch unreachable`).
- Use an external executable to send out alerts when an event occurs.

The Fabric Manager server monitors the switches that you have discovered, and you can use the Fabric Manager client to configure:

- The switches to monitor
- Global Call Home functionality

The e-mail alert from Call Home includes the following information:

- Reason for call
- Brief description of failure
- Switch(es) on which event occurred (provides name, IP address for Ethernet and Fibre Channel, and WWN)
- Firmware version
- Switch status and state

The Call Home e-mail alert will contain an attachment that includes the following information:

- Detailed switch information
- The 100 most recent events from the event log

Configure Call Home

To configure Call Home, perform the following steps:

1. From the **Tools** menu, select **Call Home**. The **Call Home** window opens (Figure 11-1).

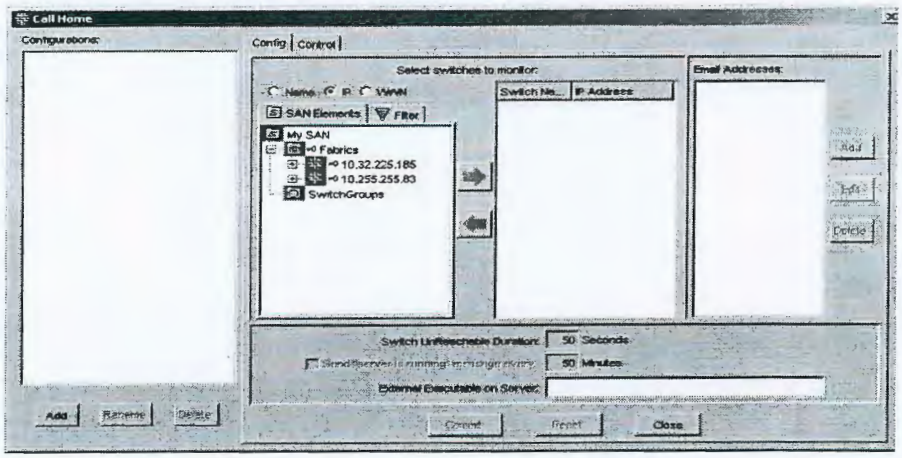


Figure 11-1 Call Home Window

2. From the **SAN Elements** tab, select the switches that you want to monitor with Call Home and click the right arrow to move them to the central window.
3. Under the **Configurations** field on the left-hand side of the display, click **Add**. A **Call Home** dialog box opens.

   You do not need to include any e-mail addresses if you opt to configure an external executable (step 9).

   ---

4. In the **Enter a configuration name field**, enter a name for your new configuration and click **OK**.

   Call Home configurations act independently of each other. No configuration ever impacts another configuration.

   ---

5. In the **E-mail Addresses** partition of the display, click **Add**. A **Call Home** dialog box opens.

6. In the **Enter an e-mail address** field, enter the e-mail address that you want Call Home to send mail to when an event occurs.
7. In the **Switch UnReachable Duration** field, enter how long (in seconds) the server must fail to contact the switch before Call Home sends an e-mail alert. The duration defaults to 50 seconds. Fabric Manager does not accept a value less than 40 seconds.
8. (Optional) Select the checkbox to prompt the server to send you a *server is running* message at intervals, and configure the time interval between messages. These messages let you know that Call Home continues to function properly. The interval defaults to one minute. Fabric Manager does not accept a value of less than one minute.
9. (Optional) In the **External Executable on Server** field, enter a path to an executable that resides on the Fabric Manager server to run that script when Call Home sends an e-mail alert. For more information, refer to *Call Home Executable Requirements* on page J-2.
10. Click **Commit**.

You cannot commit a configuration until you add at least one switch (step 2) and either one e-mail address (step 5) or the path of an external executable (step 9).

Edit Configurations

At any time you can edit a Call Home configuration. Any change that you make applies at the moment you commit the change. To edit a Call Home configuration, perform the following steps:

1. From the **Tools** menu, select **Call Home**. The **Call Home** window opens.
2. Click a configuration in the **Configurations** field.
3. Perform any of the following changes:
   - Click **Rename** to change the name the configuration.
   - Click **Delete** below the **Configurations** field to delete the configuration.
   - Add or remove switches from the **Select Switches to monitor** field.
   - Add, edit, or remove e-mail addresses from the **E-mail Addresses** field.
   - Reconfigure the **Switch UnReachable Duration** field.
   - Reconfigure the **Send "server is running" message every** options.
   - Configure an external executable

   At any point before you commit changes, you can click **Reset** to undo all the changes that you made since you last committed the configuration.
4. Click **Commit**.

Globally Enable or Disable Call Home

To globally enable or disable Call Home, perform the following steps:

1. From the **Tools** menu, select **Call Home**.
2. Click the **Control** tab.
3. Click **Enable** or **Disable**. This action processes on the server immediately.

Fabric Manager enables Call Home by default on the Fabric Manager server. However, you must configure the client to select fabrics to monitor before the Call Home server can monitor switches.